

INTRODUCTION TO THE THEORY OF NUMBERS

INTRODUCTION TO THE THEORY OF NUMBERS

LEONARD EUGENE DICKSON



THE UNIVERSITY OF CHICAGO PRESS
CHICAGO · ILLINOIS

THE UNIVERSITY OF CHICAGO PRESS, CHICAGO 37
Cambridge University Press, London, N.W. 1, England
W. J. Gage & Co., Limited, Toronto 2B, Canada

 Published November 1929 Seventh Impression 1951 Composed and printed by THE UNIVERSITY OF CHICAGO PRESS, *Chicago, Illinois, U.S.A*

PREFACE

During twenty centuries the theory of numbers has been a favorite subject of research by leading mathematicians and thousands of amateurs. Recent investigations compare favorably with the older ones. Future discoveries will far surpass those of the past.

The aim of this book is not technique, but the central ideas of the subject. Topics are not abandoned just at the point when they become most interesting, but are carried to fruition with attention to both classic and recent literature. Topics are excluded if their full treatment requires results capable of proof only by intricate analytic methods. In spite of this limitation, the material presented is fairly representative of the vast literature.

The first three chapters treat divisibility, congruences, quadratic residues, and the reciprocity law. Binary quadratic forms are treated fully in four chapters without the usual restriction to integral coefficients. These chapters are interspersed with four chapters on Diophantine equations, the first of which is quite elementary, the second involves the notion of reduced binary quadratic forms, while the last two are elementary (and may be read early) but involve long chains of arguments.

The book is intended for beginners and develops the subject from first principles. College algebra is the only prerequisite except in chapter x. But there is a gradual accumulation of definitions, concepts, and notations with which the reader must become thoroughly familiar before he can profit by the second part of the book. For this reason, he should solve many of the numerous problems, which were carefully selected and are not beyond beginners.

The book contains several original results. There are many novel features in the proofs.

For suggestions on the proof-sheets, the author is under obligations to Professors E. T. Bell, A. J. Kempner, and (for chap. iv) O. E. Brown and E. B. Escott.

L. E. DICKSON

CONTENTS

CHAPTER I

FUNDAMENTAL THEOREMS ON DIVISIBILITY

Since we shall develop the elements of the theory of numbers from first principles, we devote the first few pages to facts presented in arithmetic without formal proof. Unique factorization into primes is by no means self evident, since it usually fails for numbers involving a root of an algebraic equation.

1. Greatest common divisor. A method of finding the g.c.d. of 323 and 221 consists in dividing the former by the latter to obtain the quotient 1 and remainder 102; then dividing 221 by 102 to obtain the quotient 2 and remainder 17. Since 17 divides 102, 17 is the desired g.c.d. This work is conveniently exhibited by the following equations:

$$323=221\cdot 1+102\,,\quad 221=102\cdot 2+17\,,\quad 102=17\cdot 6$$

Similarly, to find the g.c.d of any two integers a_1 and a_2, where $a_2\neq 0$, we employ equations of the type

$$(1)\quad \begin{cases} a_1=a_2q_1+a_3\,, \quad a_2=a_3q_2+a_4\,, \quad a_3=a_4q_3+a_5, \ldots, \\ a_i=a_{i+1}q_i+a_{i+2}\,, \ldots, \quad a_{n-2}=a_{n-1}q_{n-2}+a_n\,. \\ \qquad\qquad\qquad\qquad a_{n-1}=a_nq_{n-1}\,. \end{cases}$$

Here $0\leqq a_3<|a_2|$, $0\leqq a_4<a_3, \ldots$. Since the remainders $a_3, a_4, a_5, \ldots$ form a set of decreasing integers $\geqq 0$, the process leads ultimately to a remainder which is zero. Let a_{n+1} be the first zero remainder; then the equations terminate as in (1).

We readily show that a_n is the g.c.d. of a_1 and a_2. Any common divisor of a_1 and a_2 divides a_3, by the first equation (1), and therefore divides a_4, and similarly divides

$a_5, \ldots, a_{n-2}, a_{n-1}, a_n$. Conversely, any divisor of a_n divides a_{n-1} and therefore divides $a_{n-2}, \ldots, a_4, a_3, a_2, a_1$. Hence the common divisors of a_1 and a_2 coincide with the divisors of a_n.

The first two equations (1) give

$$a_3 = a_1 - q_1 a_2 , \qquad a_4 = -q_2 a_1 + (1 + q_1 q_2) a_2 ,$$

whence a_3 and a_4 are linear, homogeneous functions of a_1 and a_2 with integral coefficients. If we grant the like fact for $a_3, \ldots, a_i, a_{i+1}$, we see from the first equation of the second line of (1) that the same fact holds for a_{i+2}. This induction completes the proof of

THEOREM 1. *Any two integers that are not both zero have a unique greatest common divisor. It can be expressed as a linear, homogeneous function of them with integral coefficients.*

Let g be the g.c.d. of a and b. Then $g = ra + sb$, where r and s are integers. Also g and c have a g.c.d. G, which is a linear function of g and c and hence of a, b, and c. Similarly, G and d have a g.c.d., which is a linear function of G and d and hence of a, b, c, d. Proceeding similarly, we obtain

THEOREM 2. *Any integers $a, b, c, \ldots, l$, not all zero, have a unique greatest common divisor, which is a linear, homogeneous function of them with integral coefficients.*

2. Relatively prime integers. Two integers a and b are called *relatively prime* if their g.c.d. is unity. Then a is said to be *prime to* b. For example, 4 is prime to 9.

THEOREM 3. *If a and b are relatively prime, any common divisor of ak and b is a divisor of k.*

By Theorem 1 there exist integers s and t such that $sa + tb = 1$. Hence $s \cdot ak + tk \cdot b = k$, which proves Theorem 3

COROLLARY 1. If a and b are relatively prime, and if ak is divisible by b, then k is divisible by b.

This follows from Theorem 3 by taking b as the common divisor of ak and b.

COROLLARY 2. If a and k are both relatively prime to b, their product ak is relatively prime to b.

If also l is prime to b, then $ak \cdot l$ is prime to b. By induction we obtain

COROLLARY 3. If several integers are all prime to b, their product is prime to b.

3. Prime numbers. An integer $p > 1$ is called a *prime* if it has no integral divisors except $\pm p$ and ± 1. The only primes < 10 are 2, 3, 5, 7. An integer b which has a divisor other than $\pm b$, ± 1, is called *composite*.

Lehmer's factor table and list of primes, both to 10 million, were published by the Carnegie Institution of Washington in 1909 and 1914. They are more accurate than earlier, shorter tables.

THEOREM 4. *If a product of several integers is divisible by a prime p, at least one of the integers is divisible by p.*

For, if not, each would be relatively prime to p, and their product would be prime to p by Corollary 3.

THEOREM 5. *Every composite, positive integer N can be expressed as a product of primes in one and but one way if we do not distinguish between two arrangements of the same prime factors.*

Let p_1 be the least divisor > 1 of N. Then $p_1 < N$. Evidently p_1 is a prime. Write $N = p_1 N_1$. If N_1 is a prime, N has been expressed as a product of two primes. But if N_1 is composite, its least divisor $p_2 > 1$ is a prime. Write $N_1 = p_2 N_2$, and proceed with N_2 as before. After a finite number of such steps we obtain a factorization $N = p_1 p_2 \ldots p_n$ of N into primes.

Suppose that $N = q_1 q_2 \ldots q_r$ is a second factorization of N into primes. By Theorem 4, the prime q_1 divides one of the primes p_i, say p_1. Hence $q_1 = p_1$, and

$$q_2 q_3 \ldots q_r = p_2 p_3 \ldots p_n .$$

Similarly, q_2 is equal to one of the factors on the right, say p_2. Proceeding in this manner, we conclude that $r=n$ and that $q_1, \ldots, q_n$ are identical in some order with $p_1, \ldots, p_n$.

4. Infinitude of primes. Euclid proved in his *Elements* that the number of primes is infinite. Given a prime p, we are to prove that there exists a prime $>p$. Let π denote the product of all the primes $\leqq p$. If $1+\pi$ is a prime it is the desired prime $>p$. But if $1+\pi$ is composite, it is a product of primes by Theorem 5. Since each of $2, 3, \ldots, p$ is a divisor of π, it is not a divisor of $1+\pi$. Hence any prime factor of $1+\pi$ exceeds p and is the desired prime.

EXERCISES 1

1. One of any three consecutive integers is divisible by 3.
2. Hence $n(n+1)(2n+1)$ is divisible by 6.
3. If 2^n+1 is a prime, n is a power of 2.
4. If 2^p-1 is a prime, p itself is a prime.
5. If p and q are distinct primes, the divisors of p^2q^3 coincide with the $3 \cdot 4$ terms of the expansion of the product

$$(1+p+p^2)(1+q+q^2+q^3) .$$

Why is this product the sum of the 12 divisors of p^2q^3?

6. Generalize Ex. 5 and prove that the number of divisors of $m=p_1^{e_1} \ldots p_k^{e_k}$ is $(e_1+1) \ldots (e_k+1)$, while their sum and the sum of their nth powers are, respectively,

$$\prod_{i=1}^{k} \frac{p_i^{e_i+1}-1}{p_i-1} \qquad \prod_{i=1}^{k} \frac{p_i^{n(e_i+1)}-1}{p_i^n-1} .$$

7. A positive integer is called a *perfect* number if it is equal to the sum of all its divisors other than itself (hence it is half of the sum of all divisors). Prove that $2^{p-1}(2^p-1)$ is a perfect number when 2^p-1 is a prime (Euclid). Verify that the first four perfect numbers are 6, 28, 496, and 8,128.

8. Every even perfect number is of Euclid's type. Hints: Let $2^{n-1}q$ be perfect, where q is odd and $n>1$. Then $2^n q=(2^n-1)s$, where s is the sum of all divisors of q. Write $s=q+d$. Then $q=d(2^n-1)$, and d is a divisor of q. Also, $d\neq q$. Hence q and d are the only divisors of q, whence $d=1$ and q is a prime 2^n-1. See Ex. 4.

9. Find the number N of integral solutions of $x^2-y^2=P>0$. Write $u=x+y$, $v=x-y$. Prove that $N=0$ if P is double an odd integer; while N is the double of the number of divisors of P or of $\frac{1}{4}P$, according as P is odd or a multiple of 4.

10. Ex. 9 implies that N is double the difference between the number of even divisors of P and the number of odd divisors.

11. There are infinitely many primes $6n-1$. Hint: Use $\pi-1$, with π as in § 4.

12. There are infinitely many primes $4n-1$. (Use $2\pi-1$.)

5. Congruent numbers. If the difference of two integers a and b is divisible by m, we shall say that a and b are *congruent modulo m* and shall employ the notation due to Gauss:

$$a\equiv b \pmod{m} .$$

The sign $\not\equiv$ denotes not congruent (incongruent). For example,

$$12\equiv 2,\ -2\equiv 3 \pmod 5 ,\quad 7\not\equiv 3 \pmod 5 .$$

If two numbers are congruent to a third, they are congruent to each other.

THEOREM 6. *If $a\equiv b$ and $c\equiv d$ (mod m), then $a+c\equiv b+d$, $a-c\equiv b-d$, $ac\equiv bd$ (mod m).*

Since $a-b$ and $c-d$ are multiples of m, their sum and difference are multiples of m. Also, $ac\equiv bc\equiv bd \pmod m$.

While $a\equiv b \pmod m$ implies $na\equiv nb \pmod m$, the converse need not hold. For example, $4\cdot 7\equiv 4\cdot 2 \pmod{10}$, $7\not\equiv 2 \pmod{10}$. But $7\equiv 2 \pmod 5$. This illustrates

THEOREM 7. *If $na\equiv nb$ (mod m) and if g is the greatest common divisor of n and m, then $a\equiv b$ (mod m/g).*

We have $n=gN$, $m=gM$, where N and M are relatively prime integers. Since $n(a-b)$ is divisible by m, $N(a-b)$ is divisible by M. Hence $a-b$ is divisible by M by Cor. 1 of § 2.

The case $g=1$ yields the important

THEOREM 8. *If $na \equiv nb \pmod{m}$ and if n is prime to m, then $a \equiv b \pmod{m}$.*

6. Least residues. When m is given, any integer k may be expressed in the form $qm+r$, where $0 \leqq r < m$. This r is called the *least residue* of k modulo m. Hence $0, 1, \ldots, m-1$ form a complete set of least residues modulo m.

THEOREM 9. *If a and $b>0$ are relatively prime and r is any integer, the least residues modulo b of*

$$(2) \qquad r, \quad a+r, \quad 2a+r, \quad \ldots, \quad (b-1)a+r$$

are $0, 1, \ldots, b-1$ rearranged.

Since there are b numbers (2), we need only prove that no two of them have the same least residue. When $0 \leqq s < b$, $0 \leqq t < b$, let $sa+r$ and $ta+r$ have the same least residue. Then $sa \equiv ta \pmod{b}$. By Theorem 8, $s \equiv t \pmod{b}$. Hence $s=t$.

7. Fermat's theorem.

THEOREM 10. *If p is a prime and a is not divisible by p, then*

$$(3) \qquad a^{p-1} \equiv 1 \pmod{p} .$$

For $r=0$, Theorem 9 states that $a, 2a, \ldots, (b-1)a$ are congruent modulo b to $1, 2, \ldots, b-1$ rearranged. By Theorem 6, the product of the numbers in the first set is congruent to that for the second set:

$$a^{b-1} \cdot 1 \cdot 2 \cdots (b-1) \equiv 1 \cdot 2 \cdots (b-1) \pmod{b} .$$

For the case in which b is a prime p, $1 \cdot 2 \cdots (b-1)$ is relatively prime to b and may be deleted from the two

members of the congruence by Theorem 8. We get (3). Fermat stated his theorem in 1640. This proof was first given by J. Ivory in 1806.

8. Euler's ϕ function. When m is a positive integer, let $\phi(m)$ denote the number of positive integers not exceeding m which are relatively prime to m. Thus $\phi(1)=\phi(2)=1$, $\phi(3)=\phi(4)=2$.

THEOREM 11. *If a and b are relatively prime positive integers,*

$$(4) \qquad \phi(ab)=\phi(a)\cdot\phi(b) .$$

The integers $\geqq 0$ and $<ab$ are given without repetition by $aq+r$ for $r=0, 1, \ldots, a-1$ and $q=0, 1, \ldots, b-1$. Evidently $aq+r$ is prime to a if and only if r is prime to a. Let r_1 be a fixed one of these $\phi(a)$ integers r. Then

$$r_1, \quad a+r_1, \quad 2a+r_1, \ldots, \quad (b-1)a+r_1$$

include exactly $\phi(b)$ numbers prime to b by Theorem 9. This proves that each of the $\phi(a)$ numbers r of type r_1 yields exactly $\phi(b)$ numbers $aq+r$ which are prime to both a and b and hence to ab. But there are $\phi(ab)$ such numbers $aq+r$. This proves (4).

We next prove that, when p is a prime,

$$(5) \qquad \phi(p^e)=p^e(1-1/p) .$$

Of the positive integers not exceeding p^e, those not prime to p^e are evidently the multiples of p, viz.,

$$p, \qquad 2p, \qquad 3p, \ldots, \qquad p^{e-1}\cdot p .$$

Hence $\phi(p^e)=p^e-p^{e-1}$. From (4) and (5) follows

THEOREM 12. *If $p_1, \ldots, p_k$ are the distinct prime factors of m,*

$$(6) \qquad \phi(m)=m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right) .$$

9. Euler's generalization of Fermat's theorem.

THEOREM 13. *If a is prime to m and $m>0$,*

$$a^{\phi(m)} \equiv 1 \pmod{m} . \tag{7}$$

Let the $n=\phi(m)$ positive integers which are prime to m and are not greater than m be denoted by

$$a_1, a_2, \ldots, a_n . \tag{8}$$

If a is prime to m, we shall prove that the products

$$aa_1, aa_2, \ldots, aa_n \tag{9}$$

are congruent modulo m to the numbers (8) rearranged. For example, if $m=8$, $a=3$, the numbers (8) are 1, 3, 5, 7, while

$$3\cdot1\equiv3 , \quad 3\cdot3\equiv1 , \quad 3\cdot5\equiv7 , \quad 3\cdot7\equiv5 \pmod{8} .$$

Each aa_i is prime to m and hence is congruent modulo m to some number (8). If $aa_i\equiv aa_j \pmod{m}$, then $a(a_i-a_j)$ is divisible by m and the same is true of a_i-a_j, whence $a_i=a_j$.

Hence the product of the numbers (8) is congruent modulo m to the product of the numbers (9). By Theorem 8, the common factor $a_1a_2\ldots a_n$ may be deleted from the two products since it is prime to m. We obtain (7), which becomes $3^4\equiv1$ (mod 8) in the example. Euler announced his theorem in 1760.

EXERCISES II

1. If p is a prime and a is any integer, $a^p\equiv a \pmod{p}$.
2. Prove Ex. 1 by expanding $(1+1+\ldots+1)^p$.
3. Any integer n is congruent modulo 9 to the sum s of its digits, since $10^k\equiv1$ (mod 9). Replacing n by s is called "casting out of nines."
4. If p is a prime, $\phi(1)+\phi(p)+\phi(p^2)+\ldots+\phi(p^e)=p^e$.

5. Hence by using Ex. I, 5, 6, show that $\Sigma\phi(d)=m$, where d ranges over all divisors of m.

6. If P is the product of the distinct prime factors common to m and n, then $\phi(mn)=P\phi(m)\phi(n)/\phi(P)$.

7. The number of irreducible fractions not greater than 1 and having denominators not greater than n is $\phi(1)+\ldots+\phi(n)$.

8. If $n>1$, the sum of the positive integers less than n and prime to n is $\frac{1}{2}n\,\phi(n)$.

9. If a is prime to m, $ax\pm my=c$ has the solution $x=ca^k$, $y=\mp cq$, where $k=\phi(m)-1$ and q is the integral quotient of $a^{\phi(m)}-1$ by m

10. Verify the following cases in which $a^n\equiv a \pmod n$ with n not a prime. $a=2$, $n=11\cdot 31$ $(2^{10}\equiv 1)$, $n=19\cdot 73$, $n=23\cdot 89$, $n=37\cdot 73$, $n=31\cdot 151$, $n=3\cdot 5\cdot 43$, $n=3\cdot 11\cdot 17$, $n=7\cdot 13\cdot 19$, $a=3$, $n=7\cdot 13(3^6\equiv 1)$, $n=11^2(3^5\equiv 1)$, $n=11^2\cdot 31$, $n=11^2\cdot 61$; $a=19$, $n=13^2$ or $13^2\cdot 7^2$, $a=18$, $n=7^3\cdot 19\cdot 37^2$.

11. Prove the following true converse of Fermat's theorem: If a^x-1 is divisible by n when $x=n-1$, but not when x is a factor $<n-1$ of $n-1$, then n is a prime Hint. If n were composite, $\phi(n)<n-1$, and $a^g\equiv 1 \pmod n$, where g is the g.c d. of $n-1$ and $\phi(n)$ and hence is a linear combination of them

CHAPTER II

THEORY OF CONGRUENCES

In this chapter we shall treat topics which are not only essential to all parts of the theory of numbers, but are required in various other branches of mathematics.

10. Definition of roots of congruences. Let the coefficients of

$$(1) \qquad f(x)=a_0x^r+a_1x^{r-1}+\ldots+a_r\equiv 0 \pmod{m}$$

be integers not all divisible by m. If c is an integer such that $f(c)$ is divisible by m, c is called a *root* of the congruence (1).

If $k\equiv c \pmod{m}$, Theorem 6 shows that $f(k)\equiv f(c)\equiv 0 \pmod{m}$, whence also k is a root of (1). But such congruent roots are identified in counting the number of distinct roots. For example, $x^2\equiv 1 \pmod{5}$ has only two roots $x\equiv 1$ or $4 \pmod{5}$.

If a_0 is not divisible by m, (1) is said to be a congruence of degree r. But $12x^3+2x^2+x-3\equiv 0 \pmod{4}$ is of degree 2.

11. Linear congruence. In a congruence of the first degree,

$$(2) \qquad ax\equiv l \pmod{m},$$

a is not divisible by m. In case a is prime to m, (2) has one and only one root. For, by multiplying each member by a power of a and applying Theorem 13, we get

$$(3) \qquad x\equiv la^e \pmod{m}, \quad e=\phi(m)-1.$$

A second method employs the existence (§ 2) of integers s and t such that $sa+tm=1$, whence $x\equiv sl \pmod{m}$.

Next, let a and m have the g.c.d. g. If l is not divisible

by g, (2) evidently has no root. Suppose, however, that l is divisible by g and write

$$a=gA\ ,\ l=gL\ ,\ m=gM\ .$$

Then (2) requires that

$$Ax\equiv L \pmod{M}\ . \tag{4}$$

Since A and M are relatively prime, there is a single root X of (4). The integers satisfying (4) are all of the form $x=X+kM$. For every integral value of k, this x satisfies (2). But $X+kM$ and $X+k'M$ are congruent modulo m (and count as the same root) if and only if $(k-k')M$ is divisible by $m=gM$, and hence if $k\equiv k' \pmod{g}$. We therefore restrict k to the values $0, 1, \ldots, g-1$. This proves

THEOREM 14. *The congruence $ax\equiv l \pmod{m}$ has no root or g roots, according as the greatest common divisor g of a and m is not or is a divisor of l. In the second case, there are exactly g roots, viz.,*

$$X,\quad X+\frac{m}{g},\quad X+2\frac{m}{g},\ \ldots,\quad X+(g-1)\frac{m}{g} \tag{5}$$

where X is the unique root of

$$\frac{a}{g}x\equiv\frac{l}{g} \left(\mathrm{mod}\ \frac{m}{g}\right)\ . \tag{6}$$

For example, consider $12x\equiv 8 \pmod{20}$. Then $g=4$ and (6) is $3x\equiv 2 \pmod{5}$, whose root is $X=4$. Hence $x\equiv 4$, 9, 14, 19 (mod 20).

12. Chinese remainder theorem.

THEOREM 15. *If $m_1, \ldots, m_t$ are relatively prime in pairs, there exist integers x for which simultaneously*

$$x\equiv a_1 \pmod{m_1},\ \ldots,\ x\equiv a_t \pmod{m_t}\ . \tag{7}$$

All such integers x are congruent modulo $m=m_1m_2\ldots m_t$.

Set $m=m_1M_1= \dots =m_tM_t$. Then M_1 is prime to $m_1, \dots, M_t$ is prime to m_t. Hence we can determine integers $\mu_1, \dots, \mu_t$ such that

$$M_1\mu_1\equiv 1 \pmod{m_1}, \dots, M_t\mu_t\equiv 1 \pmod{m_t} .$$

Then congruences (7) are all satisfied if

$$x=M_1\mu_1a_1+ \dots +M_t\mu_ta_t .$$

In fact, since $M_2, \dots, M_t$ are all divisible by m_1,

$$x\equiv M_1\mu_1a_1\equiv a_1 \pmod{m_1} .$$

Similarly, $x\equiv M_t\mu_ta_t\equiv a_t \pmod{m_t}$.

The difference between two solutions of (7) is divisible by $m_1, \dots, m_t$ and hence by their product m.

EXERCISES III

1. Find the least two positive integers having the remainders 2, 3, 2 when divided by 3, 5, 7, respectively. Answer: 23 and 128 by Sun-Tsŭ, first century A.D.

2. Find a number having the remainders 5, 4, 3, 2 when divided by 6, 5, 4, 3, respectively (Brahmegupta, seventh century).

3. Find a multiple of 7 which has the remainder 1 when divided by 2, 3, 4, 5, or 6 (Ibn al-Haitam, about 1000 A.D.)

4. If a number is expressible in each of the forms $m_in_i+a_i$ $(i=1, \dots, t)$, it is of the form $mn+x$, where x is determined modulo $m=m_1 \dots m_t$, with $m_1, \dots, m_t$ relatively prime.

5. If L is prime to M, an integer x can be chosen so that $L+Mx$ is relatively prime to any assigned integer n Hints: Let $p_1, \dots, p_k$ be the distinct prime factors of n. Take $x_i=0$ or 1, according as L is not or is divisible by p_i. Then $L+Mx_i$ is not divisible by p_i Choose $x\equiv x_1 \pmod{p_1}, \dots, x\equiv x_k \pmod{p_k}$

13. Number of roots of a congruence.

THEOREM 16. *If $m_1, \dots, m_t$ are relatively prime in pairs and m is their product, the number of roots of* (1) *is the product of the numbers of roots of*

(8) $\quad f(x)\equiv 0 \pmod{m_1}, \dots, f(x)\equiv 0 \pmod{m_t}$.

Every root of (1) is a root of each congruence (8) and hence gives a unique set of roots of them. Conversely, if $a_1, \ldots, a_t$ are roots of the respective congruences (8), and if x is found from (7), then x is a root of (1) since $f(x) \equiv f(a_i) \equiv 0 \pmod{m_i}$.

Take $m_1, \ldots, m_t$ as the powers of the distinct primes dividing m. Hence the study of congruences is reduced to the case of a power of a prime as modulus.

THEOREM 17. *Let p be a prime not dividing c. If $p>2$, the number of roots of*

$$(9) \qquad x^2 \equiv c \pmod{p^n}$$

is the same as the number (0 or 2) of roots when $n=1$. If $p=2$, $n \geqq 3$, there is no root or are just four roots, according as $c \not\equiv 1$ or $c \equiv 1 \pmod 8$. If $p=2$, $n=2$ there is no root or are two roots, according as $c \equiv 3$ or $c \equiv 1 \pmod 4$.

Let $p>2$, $n \geqq 2$. Each root of (9) satisfies

$$(10) \qquad x^2 \equiv c \pmod{p^{n-1}} .$$

Hence if ξ ranges over the roots of (10), every root of (9) is included among the numbers

$$(11) \qquad \xi + sp^{n-1} \qquad (s=0, 1, \ldots, p-1) .$$

Such a number is actually a root of (9) if and only if $q+2s\xi \equiv 0 \pmod p$, where $\xi^2 = c+p^{n-1}q$. Since 2ξ is prime to p, this linear congruence determines s uniquely.

Let $p=2$, $n \geqq 3$, and c be odd. If (9) is solvable, then x is odd and $1 \equiv x^2 \equiv c \pmod{2^3}$. Conversely, let $c \equiv 1 \pmod 8$. Then if (9) has at least one root r, it has exactly four roots x. For, x and r are odd and $(x-r)(x+r) \equiv 0 \pmod{2^n}$. Thus $\frac{1}{2}(x-r)$ and $\frac{1}{2}(x+r)$ are integers whose product is divisible by 2^{n-2} and whose difference r is odd; hence one of them is odd and the other is divisible by 2^{n-2}. Thus $x \equiv \pm r \pmod{2^{n-1}}$, whence

$$(12) \qquad x \equiv \pm r \text{ or } \pm(r+2^{n-1}) \pmod{2^n} .$$

These four numbers are incongruent modulo 2^n and are roots of (9). In other words, the 2^{n-1} odd, positive integers $x<2^n$ separate into 2^{n-3} sets of four such that the squares of those in the same set have the same positive residue $c<2^n$, while those in different sets yield different residues. Since we therefore reach 2^{n-3} distinct residues c, and since there are in all 2^{n-3} integers c for which $0<c<2^n$ and $c\equiv 1 \pmod 8$, the process yields every such c.

The number of roots of $x^2\equiv c \pmod M$ can be found by Theorems 16 and 17. See Theorems 60 and 63.

14. Congruence with a prime modulus p. Let

$$f(x)=cx^r+\ldots\equiv 0\,,\quad c\not\equiv 0 \pmod p\,, \tag{13}$$

have the root α. By the algebraic division of $f(x)$ by $x-\alpha$ we obtain a quotient $f_1(x)$ of degree $r-1$ and a remainder $r_1=f(\alpha)$ which is divisible by p. Thus

$$f(x)=(x-\alpha)f_1(x)+r_1\,,\qquad r_1\equiv 0 \pmod p\,.$$

If (13) has the root β, where $\beta\not\equiv\alpha \pmod p$, then

$$0\equiv f(\beta)\equiv(\beta-\alpha)f_1(\beta)\qquad \pmod p\,.$$

Hence $f_1(\beta)\equiv 0$ and β is a root of $f_1(x)\equiv 0 \pmod p$. Applying to the latter congruence the foregoing argument, we see that

$$f_1(x)=(x-\beta)f_2(x)+r_2\,,\qquad r_2\equiv 0 \pmod p\,.$$

Hence

$$f(x)=(x-\alpha)(x-\beta)f_2(x)+r_2(x-\alpha)+r_1\,.$$

Proceeding similarly, we see that if (13) has exactly n incongruent roots $\alpha, \beta, \ldots, \lambda$, then

$$f(x)=(x-\alpha)(x-\beta)\ldots(x-\lambda)\,f_n(x)+pF_n(x)\,, \tag{14}$$

identically in x, where f_n and F_n are polynomials having integral coefficients. The leading coefficients of $f_1, \ldots, f_r$ are $c \not\equiv 0 \pmod{p}$. In particular, this proves

THEOREM 18. *For a prime modulus, a congruence of degree r has at most r incongruent roots.*

If it has r distinct roots $\alpha, \ldots, \lambda$, then

$$(15) \qquad f(x) = c(x-\alpha)(x-\beta) \ldots (x-\lambda) + pF_r(x) ,$$

identically. For example, Fermat's theorem now gives

$$(16) \qquad x^{p-1} - 1 = (x-1)(x-2) \ldots (x-p+1) + pF(x) .$$

This identity was given by Lagrange in 1773. It proves

THEOREM 19. *If s_j is the sum of the products of $1, \ldots, p-1$ taken j at a time, then*

$$s_j \equiv 0 \ (j < p-1), \quad s_{p-1} \equiv -1 \pmod{p} .$$

Multiple roots are readily treated. Any root of $f_n(x) \equiv 0 \pmod{p}$ in (14) is a root of (13) and hence occurs among $\alpha, \ldots, \lambda$. Treating f_n as we did f, we ultimately get

$$(17) \quad f(x) = (x-\alpha)^a (x-\beta)^b \ldots (x-\lambda)^l q(x) + pR(x) ,$$

identically in x, where q and R are polynomials with integral coefficients, and $q(x) \equiv 0 \pmod{p}$ has no root. We call α a *root of multiplicity* a of $f(x) \equiv 0 \pmod{p}$.

THEOREM 20. *When the modulus is a prime, a congruence of degree r has at most r roots, a root of multiplicity m being counted as m roots.*

In case $f(x) \equiv 0$ has exactly r such roots, $q(x)$ in (17) is the constant c.

EXERCISES IV

1. Theorem 19 includes Wilson's theorem: If p is a prime, then $1 + 1 \cdot 2 \cdot 3 \ldots (p-1)$ is divisible by p. Prove the converse

2. If p is a prime $4n+1$, then $(2n)!$ is a root of $x^2 \equiv -1 \pmod{p}$. Use Wilson's theorem.

3. Each of $x^2 \equiv -1 \pmod{65}$, $x^2 \equiv -2 \pmod{33}$ has four roots.

4. Generalize the proof of Theorem 17 and show that if ξ is a root of $f(x) \equiv 0 \pmod{p^{n-1}}$, (11) is a root of $f(x) \equiv 0 \pmod{p^n}$ if and only if $sf'(\xi) \equiv -f(\xi)/p^{n-1} \pmod{p}$. Hence to each root ξ corresponds a single root of the latter if $f'(\xi) \not\equiv 0 \pmod{p}$, but either no root or p roots if $f'(\xi) \equiv 0 \pmod{p}$, whence p divides the discriminant of $f(x)$.

5. Prove that Theorem 16 holds when f is a polynomial in several variables.

6. Extend Ex. 4 to $f(x_1, \ldots, x_k)$.

15. Theorem 21. *If p is a prime and d is a divisor of $p-1$, there are exactly d roots of*

$$x^d \equiv 1 \pmod{p} . \tag{18}$$

We employ the algebraic identity

$$x^{p-1} - 1 = (x^d - 1)Q(x) ,$$

where $Q(x)$ is a polynomial of degree $t = p-1-d$ with integral coefficients. Since $Q(x) \equiv 0 \pmod{p}$ has at most t roots by Theorem 18, while, by (16), $x^{p-1} - 1 \equiv 0$ has exactly $p-1$ roots, (18) has at least $p-1-t=d$ roots. By Theorem 18, (18) has at most d roots; hence it has exactly d roots.

16. Belonging to exponent. Let a be prime to m. By Euler's theorem, $a^n \equiv 1 \pmod{m}$ when $n = \phi(m)$. If e be the least positive integer such that $a^e \equiv 1 \pmod{m}$, a is said to *belong to the exponent e modulo m*. For example, -1, 2, and 3 belong to the respective exponents 2, 3, and 6 modulo 7.

THEOREM 22. *If a belongs to the exponent e modulo m, then $a^s \equiv a^t \pmod{m}$ if and only if $s \equiv t \pmod{e}$.*

We may assume that $s \geqq t$. Write $s-t=eq+r$, $0 \leqq r < e$. Since a is prime to m,

$$1 \equiv a^{s-t} \equiv (a^e)^q a^r \equiv a^r \pmod{m} , \qquad r = 0 .$$

The case $t=0$ yields

THEOREM 23. *If a belongs to the exponent e modulo m. then* $a^s \equiv 1 \pmod{m}$ *if and only if s is divisible by e.*

In view of Euler's Theorem 13, e is a divisor of $\phi(m)$.

THEOREM 24. *If a and b belong to relatively prime exponents e and f modulo m, then ab belongs to the exponent ef modulo m.*

Let ab belong to the exponent g modulo m. Then

$$(ab)^g \equiv 1 \ , \quad 1 \equiv a^{eg} b^{eg} \equiv b^{eg} \pmod{m} \ .$$

By Theorem 23, eg is divisible by f. Hence g is divisible by f. Similarly, g is divisible by e. Hence g is divisible by ef. Thus $g \geqq ef$. But $g \leqq ef$ since

$$(ab)^{ef} = (a^e)^f (b^f)^e \equiv 1 \pmod{m} \ .$$

Hence $g = ef$ and the theorem is proved.

Let the modulus be a prime p. Then the exponent to which an integer belongs is a divisor of $\phi(p) = p-1$.

THEOREM 25. *There exist exactly* $\phi(e)$ *incongruent numbers modulo p (a prime) which belong to any given divisor e of* $p-1$ *as exponent.*

First, let $e = q^k$, where q is a prime. By Theorem 21,

$$x^{q^k} \equiv 1 \pmod{p} \tag{19}$$

has q^k distinct roots. Let the root x_1 belong to the exponent e_1. By Theorem 23, e_1 is a divisor of q^k and hence is a power of q. If $e_1 < q^k$, x_1 is therefore one of the $d = q^{k-1}$ roots of $x^d \equiv 1 \pmod{p}$. There are $q^k - q^{k-1} = \phi(q^k)$ roots of (19) which do not satisfy the latter congruence. Each such root belongs to the exponent q^k.

Let e be any divisor of $p-1$. Express e as a product of powers of distinct primes. By Theorem 24 and the case

just treated, we conclude that there exists an integer a belonging to the exponent e. Then no two of the e numbers

$$1, a, a^2, \ldots, a^{e-1}$$

are congruent modulo p in view of Theorem 22. Hence they give all the roots of $x^e \equiv 1 \pmod{p}$.

To prove our theorem it remains to show that a root a^n belongs to the exponent e if and only if n is prime to e. First, if n be prime to e, then $(a^n)^l \equiv 1 \pmod{p}$ requires that nl be divisible by e by Theorem 23, whence l is divisible by e, and a^n belongs to the exponent e. Next, if n and e have a common divisor $d > 1$, then

$$(a^n)^{e/d} \equiv (a^e)^{n/d} \equiv 1 \pmod{p},$$

and a^n belongs to an exponent $\leqq e/d < e$.

EXERCISES V

1. If p is a prime distinct from 2 and 5, and if $0 < a < p$, the fraction a/p can be expressed as a pure circulating decimal, and the number of digits in the period is the exponent to which 10 belongs modulo p.

2. If a, b, m are relatively prime in pairs and if l is the least positive integer such that a^l is congruent to a power of b modulo m, then l divides $\phi(m)$. Hint: Employ the g.c.d. g of $l = Lg$ and $\phi(m) = qg$, and a solution k of $Lk \equiv 1 \pmod{q}$. Then $a^g \equiv a^{lk} \pmod{m}$.

3. If a is prime to $M = \Pi p_i^{n_i}$ and $a^M \equiv a \pmod{M}$, and a belongs to the exponent e_i modulo p_i, then

$$\frac{M}{p_i^{n_i}} \equiv 1 \pmod{e_i}, \qquad a^{p_i} \equiv a \pmod{p_i^{n_i}}$$

for each i. Conversely, these imply $a^M \equiv a \pmod{M}$.

17. Primitive roots. For $e = p-1$ the last theorem shows that there exist exactly $\phi(p-1)$ incongruent integers which belong to the exponent $p-1$ modulo p (a prime);

they are called *primitive roots* of p. For example, 2 and 3 are the primitive roots of 5.

Next, consider a composite modulus m. We saw that any integer a prime to m belongs to an exponent which is a divisor of $\phi(m)$. If this exponent is $\phi(m)$ itself, a is called a primitive root of m. Which numbers m possess primitive roots?

Let $m = m_1 m_2 \dots m_k$, where $m_1, \dots, m_k$ are powers of distinct primes. Let l be the least common multiple of $\phi(m_1), \dots, \phi(m_k)$. By Euler's theorem, $a^{\phi(m_i)} \equiv 1 \pmod{m_i}$, whence $a^l \equiv 1$. Since $a^l - 1$ is divisible by each m_i, it is divisible by their product m.

When p is a prime, $\phi(p^n) = p^{n-1}(p-1)$ is even if $p > 2$ and if $p = 2$, $n \geqq 2$. Thus $\phi(p^n)$ is even if $p^n > 2$. Hence if two of our m_i exceed 2, the least common multiple l of $\phi(m_1), \dots, \phi(m_k)$ is less than their product $\phi(m)$. Then there exist no primitive roots of m since $a^l \equiv 1 \pmod{m}$.

Let therefore no two of our m_i exceed 2. Then m is either a power of a prime $\geqq 2$ or the double of a power of an odd prime.

Evidently 3 is a primitive root of 2^2. But there is no primitive root of 2^n, $n \geqq 3$. For, when a is odd,

$$a^2 = 1 + 8b, \qquad a^4 = 1 + 16c, \dots, \qquad a^{2^{n-2}} = 1 + 2^n h,$$
$$2^{n-2} = \tfrac{1}{2}\phi(2^n).$$

To show there exist primitive roots of p^n, where p is an odd prime, start with any primitive root ρ of p. By Fermat's theorem, $\rho^p - \rho$ is a multiple σp of p. Take any integer t such that $\sigma - t$ is not divisible by p. Employ $r = \rho + pt$, which is a primitive root of p such that

(20) $\qquad r^{p-1} - 1$ is not divisible by p^2.

In fact, the binomial theorem gives

$$r^p \equiv \rho^p \pmod{p^2}, \quad r^p - r \equiv p(\sigma - t) \not\equiv 0 \pmod{p^2}.$$

Thus $r^{p-1}=1+kp$, where k is not divisible by p. By the binomial theorem,

(21) $$(1+kp^j)^p \equiv 1+kp^{j+1} \pmod{p^{j+2}}\ ,\ j \geqq 1\ .$$

The case $j=1$ shows that

(22) $$(r^{p-1})^{p^s} \equiv 1+kp^{s+1} \pmod{p^{s+2}}$$

holds when $s=1$. Granting (22) for a certain s, and applying (21) with $j=s+1$, we conclude that (22) holds when s is replaced by $s+1$. Hence (22) holds for every s. For $s=n-2$, it gives

$$r^f \equiv 1+kp^{n-1} \not\equiv 1 \pmod{p^n}\ ,\quad f=(p-1)p^{n-2}$$

Let r belong to the exponent e modulo p^n. Then e divides $\phi(p^n)=(p-1)p^{n-1}$. But e is a multiple of $p-1$, since $r^e \equiv 1 \pmod{p}$ and r is a primitive root of p. If $e<\phi(p^n)$, e would divide f, whence $r^f \equiv 1 \pmod{p^n}$, contrary to the preceding. Hence $e=\phi(p^n)$ and r is a primitive root of p^n

Finally, let $m=2p^n$, where p is an odd prime. Employ a primitive root r of p^n. Let g be that one of the numbers r and $r+p^n$ which is odd. If g belongs to the exponent e modulo m, then

$$r^e \equiv g^e \equiv 1 \pmod{p^n}\ ,$$

whence e is divisible by $\phi(p^n)=\phi(m)$. But $e \leqq \phi(m)$. Hence $e=\phi(m)$ and g is a primitive root of m.

THEOREM 26. *There exist primitive roots of m if and only if m is 2, 4, p^n, or $2p^n$, where p is an odd prime. If r is a primitive root of p for which* (20) *holds, then r is a primitive root of p^n.*

The least primitive roots of primes $\leqq 25{,}409$ have been tabulated.*

* *Proc. London Math Soc.*, XXI (1922), 350–58; when $p=8{,}011$ read $g=14$ for $g=13$. To 5,000 in *Acta mathematica*, XVII (1893), 315–20; XX (1896), 143–57; XXII (1899), 200. To 6,200 in Wertheim's *Anfangsgrunde der Zahlenlehre*, 1902.

EXERCISES VI

1. The least residues modulo 41 of the successive powers of 2 are 2, 4, 8, 16, 32, 23, 5, 10, 20, $40 \equiv -1$, whence 2 belongs to the exponent $2 \cdot 10$. Similarly, 3 belongs to the exponent $2 \cdot 4$. Hence 2^4 and 3 belong to the relatively prime exponents 5 and 8. Thus $2^4 \cdot 3 \equiv 7 \pmod{41}$ belongs to the exponent 40, and 7 is a primitive root of 41.

2. Find primitive roots of 7^2 and $2 \cdot 7^2$.

3. A primitive root a of p^n is a primitive root of p. Hint: Let a belong to exponent e modulo p and show that $a^k \equiv 1 \pmod{p^n}$ for $k = ep^{n-1}$.

4. A primitive root r of p is a primitive root of p^n only when (20) holds. Hint: Write $r^{p-1} = 1 + kp^S$, where k is prime to p. By (21) show that $r^t \equiv 1 \pmod{p^n}$ for $t = (p-1)p^{n-S}$. But $t < \phi(p^n)$ if $S > 1$.

5. There are $(p-1)\phi(p-1)$ primitive roots of p^n incongruent modulo p^2.

6. There are exactly $\phi\{\phi(p^n)\}$ primitive roots of p^n.

7. There are as many primitive roots of $2p^n$ as of p^n.

8. The product of all primitive roots of a prime $p > 3$ is $\equiv 1 \pmod{p}$.

18. Residual polynomials and congruences. We shall obtain interesting results which, however, are not needed later in this text.

A polynomial $f(x)$ with integral coefficients which is divisible by m for every integral value of x is called a *residual polynomial modulo m*. We then write $f(x) \equiv 0 \pmod{m}$, and call this a *residual congruence*. For example, if p is any prime, $x^p - x \equiv 0 \pmod{p}$.

Another problem is to find the polynomials with rational coefficients which have integral values for all integral values of x. Bring the coefficients to their least common denominator m. Hence this problem reduces to the former.

We readily find all residual polynomials $f(x)$ modulo p a prime. Then $f(x)\equiv 0 \pmod p$ has the roots, $0, 1, \ldots, p-1$, and (14) gives an identity

$$f(x)=Pq(x)+pG(x)\ , \quad P=x(x-1)\ldots(x-p+1)\ .$$

By (16), $x^p-x=P+pH(x)$. Elimination of P gives

$$f(x)=(x^p-x)u(x)+pv(x)\ . \tag{23}$$

This proves the case $n=1$ of

THEOREM 27. *If $n\leqq p$, every residual polynomial modulo p^n is of the form*

$$\sum_{k=0}^{n} p^{n-k}(x^p-x)^k f_k(x)\ , \tag{24}$$

where the $f_k(x)$ are polynomials with integral coefficients.

To proceed by induction on n, let the theorem hold for a certain n and prove it for $n+1\leqq p$. Let $f(x)\equiv 0 \pmod{p^{n+1}}$. Since this holds also modulo p^n, $f(x)$ is of the form (24). For any integer x, $x^p-x=py$, where y is an integer. Write $Z=y-z$. By the binomial theorem,

$$(x+pz)^p\equiv x^p=x+pz+pZ \pmod{p^2}\ ,$$

$$[(x+pz)^p-(x+pz)]^k=(pZ+tp^2)^k\equiv p^kZ^k \pmod{p^{k+1}}\ .$$

Replacing x by $x+pz$ in (24), we get

$$f(x+pz)\equiv\sum_{k=0}^{n} p^{n-k}p^kZ^kf_k(x+pz) \pmod{p^{n+1}}\ .$$

But $f(x+pz)$ is divisible by p^{n+1} for every x and every z. Hence

$$\sum_{k=0}^{n} f_k(x)Z^k\equiv 0 \pmod p$$

for every integer Z. This congruence of degree $\leqq n<p$ in Z has therefore p roots. By Theorem 18 this is impossible

unless each coefficient is divisible by p for every x. Hence each $f_k(x)$ is of the form (23). Insertion in (24) yields a result of type (24) with n replaced by $n+1$. Hence the induction is complete.

Further principles are required in the study of a general modulus m. Let $\mu=\mu(m)$ denote the least positive integer for which $\mu!$ is divisible by m. For example, $\mu(p)=p$; $\mu(p_1 \ldots p_k)=p_k$ if $p_1, p_2, \ldots, p_k$ are distinct primes in ascending order of magnitude; $\mu(p^n)=pn$ if* $n<p$.

Since the same variable x is used throughout, we do not exhibit it in the abbreviation

$$\Pi(k)=x(x-1) \ldots (x-k+1)\ , \tag{25}$$

when k is a positive integer. Since the binomial coefficient $\binom{x}{\mu}$ is an integer for every integral value of x, $\Pi(\mu)$ is divisible by $\mu!$ and hence by m. Thus

$$\Pi(\mu(m))\equiv 0 \pmod{m}\ . \tag{26}$$

In (26) we may replace m by any new integer and hence by any divisor d of m. Then multiplication by m/d yields

$$\frac{m}{d}\Pi(\mu(d))\equiv 0 \pmod{m}, \text{ if } d \text{ divides } m\ . \tag{27}$$

When $d=1$ we interpret the left member to mean m.

For example, when $m=6$ the cases $d=6, 2, 1$ yield $\mu(6)=3$, $\mu(2)=2$, and

$$x(x-1)(x-2)\equiv 0,\quad 3x(x-1)\equiv 0,\quad 6\equiv 0 \pmod{6}\ , \tag{28}$$

while $d=3$ yields $\mu(3)=3$, $2x(x-1)(x-2)\equiv 0$, which is a consequence of (28_1).

* But if $n\geqq p$, the determination of μ without trial requires a complicated computation explained by Kempner, *Amer. Math. Monthly*, XXV (1918), 209. If $P_1, \ldots, P_k$ are powers of distinct primes, $\mu(P_1 \ldots P_k)$ is the largest of $\mu(P_1), \ldots, \mu(P_k)$.

To illustrate our next problem, we shall find every $ax^2+bx+c \equiv 0 \pmod 6$. By use of $x=0, 1, -1$, we get

$$c\equiv 0,\ a+b\equiv 0,\ a-b\equiv 0,\ 2a\equiv 0 \pmod 6\ ,$$

whence $a\equiv 3A$, $b\equiv -3A \pmod 6$. Thus ax^2+bx+c is a linear combination of $3x(x-1)$ and 6.

I. Any polynomial $f(x)=\Sigma c_i x^i$ of degree n can be expressed in one and but one way in the form

$$(29)\qquad a_0+a_1x+a_2\binom{x}{2}+\cdots+a_n\binom{x}{n}\ .$$

This follows when $n=1$ by taking $a_0=c_0$, $a_1=c_1$. To proceed by induction from $n-1$ to n, we assume I for all polynomials of degree $n-1$. Then

$$(30)\qquad f(x)-n!c_n\binom{x}{n}$$

lacks x^n and hence is expressible uniquely in the form

$$(31)\qquad a_0+a_1x+\cdots+a_{n-1}\binom{x}{n-1}\ .$$

Define a_n to be $n!c_n$. Hence $f(x)$ is identical with (29).

Henceforth, let every c_i be an integer. Then

II. $\qquad a_i/i!$ is an integer for $i=0, 1, \ldots, n$.

Assume that II holds for all polynomials of degree $\leqq n-1$. Since the last part of (30) is $-c_n x(x-1)\ldots(x-n+1)$, (30) is identical with a polynomial having integral coefficients. By (31), II holds for $i\leqq n-1$. Also, $a_n/n!$ is the integer c_n. Hence the proof of II by induction is complete.

The a_i's are all integers by II.

For $x=0, 1, 2, \ldots, n$, the values of (29) are

$$a_0,\ a_0+a_1,\ a_0+2a_1+a_2,\ \ldots,\ a_0+\ldots+a_n\ .$$

If these are all divisible by m, the same is true of $a_0, a_1, \ldots, a_n$. Let α_s denote the integer a_s/m. This proves

III. Every residual polynomial modulo m is of the form

$$(32) \qquad m\alpha_0 + \sum_{k=1}^{n} A_k \Pi(k) \ , \quad A_k = m\alpha_k/k! \ ,$$

where each α_k and A_k is an integer.

We seek the least positive integer n for which $A_n = 1$, i.e., $m\alpha_n = n!$. Since $n!$ is divisible by m, the least n is $\mu(m)$. In view also of (26), this proves

IV. $\mu(m)$ is the minimum degree of a residual polynomial modulo m whose leading coefficient is unity.

Let d be any divisor of m. Then $\mu(d)$ is the least n for which $A_n = m/d$, i.e., $d\alpha_n = n!$. In view also of (27), this proves

V. If d is any divisor of m, $\mu(d)$ is the minimum degree of a residual polynomial modulo m whose leading coefficient is m/d.

Let $P = cx^n + \cdots$ be any residual polynomial of degree n modulo m. Let g denote the g.c d. of $c = gC$ and $m = gM$. Then C is prime to M, and $CL \equiv 1 \pmod{M}$ has a unique solution L. Then every integer satisfying $Cz \equiv 1 \pmod{M}$ is of the form $z = L + My$ By Ex. III, 5, we can choose an integer y so that z is prime to m. Then $zZ \equiv 1 \pmod{m}$ has a solution Z. Thus

$$cz = gCz \equiv g, \quad zP = Q \equiv gx^n + \cdots, \quad P \equiv ZQ \pmod{m} .$$

This proves

VI. Any residual polynomial modulo m is term by term congruent modulo m to the product of an integer prime to m by a residual polynomial whose leading coefficient is a divisor of m.

We shall define the chain of residual congruences modulo

m. For $m=6$, the chain is (28), with no entry for the divisor 3 since $\mu(3)=\mu(6)$. To treat also the example $m=16$, note that its divisors >1 are 16, 8, 4, 2, while $\mu(16)=6$, $\mu(8)=\mu(4)=4$, $\mu(2)=2$. When $d=16$, 8, 2, and 1, (27) gives the chain

$$(33)\quad x(x-1)\cdots(x-5)\equiv 0\,,\quad 2x(x-1)(x-2)(x-3)\equiv 0\,,\quad 8x(x-1)\equiv 0\,,\quad 16\equiv 0 \pmod{16}\,.$$

The omitted case $d=4$ leads to the double of the second congruence.

For any m we separate its divisors $d>1$ into sets such that $\mu(d)$ has the same value for all the d's of a set, but different values for d's of different sets. We discard all but the largest d of a set. Let $d_1, \ldots, d_s$ denote the divisors that remain. Arrange them so that $\mu(d_1), \ldots, \mu(d_s)$ are in order of decreasing magnitude. Then (27) with $d=d_1, \ldots, d_s$, together with $m\equiv 0$ are said to form the chain of residual congruences modulo m.

That all residual congruences are consequences of those of the chain follows from

THEOREM 28. *Every residual polynomial $f(x)$ modulo m is a sum of products of m and $m/d_i\cdot\Pi(\mu(d_i))$ for $i=1, \ldots, s$ by polynomials in x with integral coefficients.**

By VI, $f(x)=m\phi(x)+ZF(x)$, where Z and the coefficients of $\phi(x)$ are integers, while $F(x)$ is a residual polynomial modulo m of degree n in which the coefficient of x^n is m/d. If $d=1$, the term Zmx^n may be combined with $m\phi$, and $Z(F-mx^n)$ taken as the new ZF. Hence let $d>1$. Then d is in a set having a certain maximum divisor d_i of m such that $\mu(d)=\mu(d_i)$. Write Π for $\Pi(\mu(d))$. By (27)

* Due to Kempner, *Trans. Amer. Math. Soc.*, XXII (1921), 240–88, who gave a different proof. A redundant theorem permitting all $\Pi(k)$, $k=1, \ldots, \mu(m)$, had been proved by Nielsen, *Nieuw Archief voor Wiskunde* (ser. 2), X (1913), 100–106.

the products of Π by m/d and m/d_1 are $\equiv 0 \pmod{m}$. Let g be their g.c.d., which is a linear combination of them. Hence $g\Pi \equiv 0 \pmod{m}$. In $m/d_1 = gQ$, Q is an integer. Thus g is the integral quotient of m by d_1Q. By V, $\mu(d_1Q)$ is the minimum degree of a residual congruence modulo m whose leading coefficient is g. But $g\Pi \equiv 0$ is of degree $\mu(d_1)$. Hence $\mu(d_1) \geqq \mu(d_1Q)$. The latter is the least integer M such that $M!$ is divisible by d_1Q. Then $M!$ is divisible by d_1, while $\mu(d_1)$ is the least integer μ for which $\mu!$ is divisible by d_1. Hence $M \geqq \mu$. The two inequalities give $\mu(d_1Q) = \mu(d_1)$. Unless $Q=1$ this would contradict the definition of d_1 as the maximum of its set. Thus $Q=1$, and $m/d_1 = g$ is a divisor of m/d. Let q denote the integral quotient. Hence

$$(34) \qquad \frac{m}{d}\Pi(\mu(d)) = q \cdot \frac{m}{d_1}\Pi(\mu(d_1)) \; .$$

The second factor on the right is one of the functions permitted in the theorem.

We return to $F(x) = (m/d)x^n + \cdots$. By V, $n \geqq \mu(d)$. Hence the product of (34) by a power of x has the same leading term as $F(x)$. The difference is a residual polynomial modulo m of degree $< n$. We apply to it the argument made for the initial $f(x)$. Since the degree is lowered at each step, the process finally leads to a difference which is zero. Hence the theorem is proved.

If $f(x) - g(x) \equiv 0 \pmod{m}$, we call f and g *residually congruent* modulo m and write $f \equiv g \pmod{m}$.

By a *reduced system* of polynomials $r_i(x)$ modulo m, we mean a system having least coefficients $\geqq 0$ such that every polynomial with integral coefficients is residually congruent modulo m to one and only one of the r_i.

Theorem 28 shows that such a reduced system exists for every $m > 0$ and indicates the method of finding it, as will be evident from Exs. 1–4.

EXERCISES VII

1. By use of (28) show that the reduced system modulo 6 is composed of the ax^2+bx+c, where $a=0$, 1, or 2, while b and c are chosen from 0, 1, . . . , 5.

2. By (33), the reduced system modulo 16 is composed of the $ax^5+bx^4+cx^3+dx^2+ex+f$, where $a=0$. 1; $b=0$, 1; c and d are chosen from 0, 1, . . . , 7; and e and f from 0, 1, . . . , 15.

3. The chain of residual congruences modulo $3\cdot5\cdot11$ is

$$\prod_{i=0}^{10}(x-i)\equiv0,\quad 11\prod_{i=0}^{4}(x-i)\equiv0,\quad 55\prod_{i=0}^{2}(x-i)\equiv0,\quad 165\equiv0\,.$$

The reduced system is $a_{10}x^{10}+\ldots+a_0$, where $a_{10}, \ldots, a_5=0$, 1, . . . , 10; a_4, $a_3=0$, 1, . . . , 54; a_2, a_1, $a_0=0$, 1, . . . , 164.

4. Deduce Theorem 27 from Theorem 28. Hints: By (16), $P=\Pi(p)=x^p-x+pq$, $\Pi(2p)=P(P+pt)$ since $x-(p+s)\equiv x-s \pmod p$; $\Pi(3p)=\Pi(2p)(P+pr)$, etc. Show by each theorem that the reduced system modulo 7^3 is $a_{20}x^{20}+\ldots+a_0$, where $a_{20}, \ldots, a_{14}=0, \ldots, 7-1$, $a_{13}, \ldots, a_7=0, \ldots, 7^2-1$; $a_6, \ldots a_0=0, \ldots, 7^3-1$.

5. For $m=p$, 5^2, or 42, there are p^p, 5^{15}, or $2^2 3^3 7^7$ polynomials in the reduced system.

6. To which reduced polynomial is $x^6+102x^4+5x^2-23x+38$ residually congruent modulo 5, 7, 42, or 25?

7. $x^4+3x^3+25x+1$ is residually congruent modulo 30 to any $f(x)$ having $f(0)\equiv1$, $f(1)\equiv0$, $f(2)\equiv1$, $f(3)\equiv28$, $f(4)\equiv9$, $f(5)\equiv16 \pmod{30}$.

8. $g(x)=(x^p-x)^p-p^{p-1}(x^p-x)$ is a residual polynomial modulo p^{p+1}. For $n<2p+2$, every residual polynomial modulo p^n is a sum of products of

$$\phi_{n,k}=p^{n-k}(x^p-x)^k(0\leqq k\leqq n),\ g(x)\cdot\phi_{n-p-1,\,k-1}\qquad(1\leqq k\leqq n-p)$$

by polynomials in x with integral coefficients.

9. For g in Ex. 8 and $n=p^2+p+1$, $g^p-p^{p^2-1}g$ is a residual polynomial modulo p^n.

10. If $m=ABC\ldots$, where $A, B, \ldots$ are powers of distinct primes, and if g is the greatest of their exponents, then

$$x^g(x^{\phi(m)}-1)$$

is a residual polynomial modulo m. If P, Q, R, . . . are residual polynomials modulo A, B, C, . . . , respectively, then PQR . . . ,

$$\frac{m}{A}Pf_1+\frac{m}{B}Qf_2+\cdots, \qquad \frac{m}{AB}PQf_1+\frac{m}{AC}PRf_2+\cdots$$

are residual polynomials modulo m.

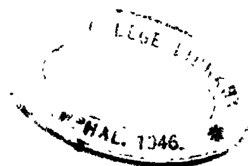
19. Indices. Let r be a primitive root of the prime p. By Theorem 22, the least residues modulo p of

$$1, r, r^2, \ldots, r^{p-2} \tag{35}$$

are $1, 2, \ldots, p-1$ rearranged. In other words, any integer N not divisible by p is congruent modulo p to one and only one of the powers (35). The exponent of this power is called the *index* of N and denoted by Ind N. Indices play a rôle similar to logarithms. We have

$$\text{Ind } NM \equiv \text{Ind } N + \text{Ind } M, \qquad \text{Ind } N^k \equiv k \text{ Ind } N \pmod{p-1}.$$

Unlike logarithms, we here require tables for each p. For $p<1{,}000$ such tables occur in Jacobi's *Canon Arithmeticus*, Berlin, 1839.



CHAPTER III

QUADRATIC RESIDUES AND RECIPROCITY LAW

The quadratic reciprocity law is doubtless the most important tool in the theory of numbers and occupies the central position in its history. Its generalizations form a leading topic, past and present, in the theory of algebraic numbers.

20. Quadratic residues. All integers prime to m are separated into two sets: those which are residues modulo m of squares are called *quadratic residues* of m, while all the remaining ones are called *quadratic non-residues* of m. In other words, an integer k prime to m is a quadratic residue or non-residue of m, according as there exist roots or no roots of the congruence $x^2 \equiv k \pmod{m}$.

For example, 1, 2, and 4 are quadratic residues of 7, while 3, 5, and 6 are non-residues of 7.

Let r be a primitive root of the odd prime p. Evidently each even power of r is a quadratic residue of p. Conversely, since a quadratic residue k is congruent modulo p to a square x^2, and since $x \equiv r^i$ by § 19, we have $k \equiv r^{2i} \pmod{p}$.

By Theorem 22, $r^s \equiv r^t \pmod{p}$ if and only if $s \equiv t \pmod{p-1}$. Since $p-1$ is even, no odd power of r is congruent to an even power of r modulo p. Hence all odd powers of r are quadratic non-residues of p.

We therefore have the following results:

THEOREM 29. *The quadratic residues of an odd prime p coincide with the residues modulo p of the even powers of a primitive root r of p; the quadratic non-residues conicide with the residues of the odd powers of r.*

THEOREM 30. *There are exactly* $\frac{1}{2}(p-1)$ *incongruent quadratic residues and* $\frac{1}{2}(p-1)$ *incongruent quadratic non-residues of* p.

THEOREM 31. *The product of two quadratic residues or two non-residues of* p *is a quadratic residue of* p. *The product of a quadratic residue and a non-residue is a non-residue.*

We next prove

THEOREM 32. *A number not divisible by* p *is a quadratic residue* R *of* p *or a non-residue* N *of* p *if and only if it satisfies the first or second of the congruences*

$$(1) \qquad R^{\pi}\equiv 1\ ,\quad N^{\pi}\equiv -1\ (mod\ p)\ ,\quad \pi=\tfrac{1}{2}(p-1)\ .$$

This follows from Theorem 29 and $r^{\pi}\equiv -1$ (mod p), which is true since

$$(r^{\pi}-1)(r^{\pi}+1)\equiv 0\ ,\quad r^{\pi}\not\equiv 1\ (\text{mod}\ p)\ .$$

EXERCISES VIII

1. By (1), -1 is a quadratic residue of any prime $4m+1$ and a non-residue of any prime $4m+3$.

2. Prove that -3 is a quadratic residue of any prime $p=3l+1$ and a non-residue of any odd prime $p=3l+2$. Hint: By Fermat's theorem decide when $(x^3-1)/(x-1)\equiv 0$ (mod p) has two roots or no root.

3. Hence find the primes of which $+3$ is a quadratic residue.

4. If a solvable congruence $x^2\equiv c$ (mod n) has k roots, there are exactly $\phi(n)/k$ quadratic residues of n, c prime to n.

5. If k is not divisible by the odd prime p and if g is the g.c.d. of n and $p-1$, then $x^n\equiv k$ (mod p) has exactly g roots or no root, according as $k^{(p-1)/g}\equiv 1$ (mod p) holds or fails.

6. For what primes p is $x^3\equiv k$ (mod p) solvable for every k?

21. Legendre's symbol. If p is an odd prime and m is any integer not divisible by p, the symbol $(m|p)$ is defined to have the value $+1$ or -1, according as m is a quadratic

residue or non-residue of p. For example, $(2|7)=1$, $(3|7)=-1$, $(-2|7)=-1$.

Theorems 31 and 32 may now be expressed compactly as follows:

$$(m|p)(n|p)=(mn|p)\ , \tag{2}$$

$$(m|p)\equiv m^{\frac{1}{2}(p-1)} \pmod{p}\ . \tag{3}$$

22. The lemma of Gauss.

THEOREM 33. *If q is not divisible by the odd prime p, and if n denotes the number of the least positive residues modulo p of*

$$q,\ 2q,\ 3q,\ \ldots,\ \tfrac{1}{2}(p-1)q \tag{4}$$

which exceed $\frac{1}{2}p$, then

$$(q|p)=(-1)^n\ . \tag{5}$$

No one of the least residues of the products (4) is zero and no two are equal by Theorem 8. Let $a_1, \ldots, a_n$ be the residues $>\frac{1}{2}p$, and $b_1, \ldots, b_k$ the residues $<\frac{1}{2}p$, whence $n+k=\frac{1}{2}(p-1)$. Evidently $p-a_1, \ldots, p-a_n$ lie between 0 and $\frac{1}{2}p$, and no two are equal; no one of them is equal to one of the b_i. For, if $p-a=b$, where a and b are the residues of αq and βq, then $(\alpha+\beta)q\equiv 0$, $\alpha+\beta\equiv 0 \pmod{p}$, whereas α and β are positive and $\leqq\frac{1}{2}(p-1)$. Hence the $\pi=\frac{1}{2}(p-1)$ numbers

$$p-a_1,\ \ldots,\ p-a_n,\quad b_1,\ \ldots,\ b_k \tag{6}$$

are distinct, positive integers $<\frac{1}{2}p$, and therefore are a rearrangement of

$$1,\ 2,\ \ldots,\ \pi\ . \tag{7}$$

Hence the product of the numbers (6) is equal to that of (7), and therefore

$$(-1)^n a_1 \cdots a_n b_1 \cdots b_k \equiv 1\cdot 2 \cdots \pi \pmod{p}\ .$$

Since the a_i and b_i together give the residues of all the numbers (4),

$$a_1 \cdots a_n b_1 \cdots b_k \equiv 1 \cdot 2 \cdots \pi \cdot q^\pi \pmod{p} .$$

Hence

$$(-1)^n \equiv q^\pi \pmod{p} .$$

The second member is congruent to $(q|p)$ by (3). This proves (5).

Gauss obtained another formula of type (5). Any positive real number x is the sum of an integral part I and a decimal part; write $[x]$ for I. Thus $[x]$ denotes the largest integer $\leq x$ For example, $[5\frac{1}{3}]=5$, $[5]=5$.

Let $r_1, \ldots, r_\pi$ denote the least residues modulo p of the $\pi=\frac{1}{2}(p-1)$ numbers (4). Then

(8) $$q=p[q/p]+r_1, \ldots, \pi q=p[\pi q/p]+r_\pi .$$

The sum of 1, 2, . . . , π is $P=\frac{1}{8}(p^2-1)$. Hence

(9) $$Pq=pM+A+B ,$$

where $A=a_1+\ldots+a_n$, $B=b_1+\ldots+b_k$, and

(10) $$M=[q/p]+[2q/p]+\ldots+[\pi q/p] .$$

Since the numbers (6) form a rearrangement of (7) their sums are equal:

$$P=pn-A+B .$$

Subtracting this from (9), we get

$$P(q-1)=p(M-n)+2A \equiv M-n \pmod{2} .$$

If q is odd, this gives $n \equiv M \pmod{2}$, and (5) yields

(11) $$(q|p)=(-1)^M \qquad (q \text{ odd}) .$$

If $q=2$, then $M=0$ and $P\equiv n \pmod{2}$, whence

(12) $$(2|p)=(-1)^{(p^2-1)/8}$$

23. The quadratic reciprocity law.

THEOREM 34. *If p and q are distinct odd primes,*

(13) $$(p|q)(q|p)=(-1)^e\ ,\quad e=\tfrac{1}{2}(p-1)\cdot\tfrac{1}{2}(q-1)\ .$$

A geometrical proof will be given in § 24. We here present Gauss's third* proof. By the symmetry of (13), we may take $q<p$. Then any term of the sum (10) is either equal to the term just preceding it or exceeds the latter by unity. The final term is equal to $Q=\frac{1}{2}(q-1)$ since

$$\frac{\pi q}{p}=\frac{(p-1)q}{2p}=Q+\frac{p-q}{2p}\ .$$

If t is one of 1, 2, . . . , Q, we seek the value of s for which

$$[sq/p]=t-1,\quad [(s+1)q/p]=t\ .$$

Since $s<p$, neither of the fractions in brackets is an integer. Hence

$$sq/p<t<(s+1)q/p\ ,$$

$$s<tp/q<s+1\ ,\quad s=[tp/q]\ .$$

Hence the number of terms (10) having the value $t-1$ is

$$[tp/q]-[(t-1)p/q]\ ,$$

while the number of terms (10) having the value Q is

$$\pi-[Qp/q]\ .$$

The sum of a number of equal terms is the product of their number by their common value. Hence

$$M=0[p/q]+1([2p/q]-[p/q])+2([3p/q]-[2p/q])+\cdots$$
$$+(Q-1)([Qp/q]-[(Q-1)p/q])+Q(\pi-[Qp/q]).$$

* His long first proof was by induction. His second proof will be given in Ex XXXVII, 6.

Hence if we write

(14) $$N=[p/q]+[2p/q]+\cdots+[Qp/q]\ ,$$

we have

(15) $$M+N=Q\pi\ .$$

Since N is derived from M by interchanging p and q, (11) gives $(p|q)=(-1)^N$. From this, (11) and (15), we get (13).

By Ex. VIII, 1,

(16) $$(-1\,|\,p)=(-1)^{\frac{1}{2}(p-1)}\ .$$

By (3) or by the definition of the symbols,

(17) $$(n|p)=(m|p)\quad \text{if } n\equiv m \pmod p\ .$$

We readily evaluate any symbol $(n|p)$ by use of (2), (12), (13), (16), and (17). For example, let $n=-22$, $p=73$; then

$$(-22|73)=(-1|73)(2|73)(11|73),\ (-1|73)=1\ ,$$
$$(2|73)=1,\ (11|73)=(73|11)=(7|11)=-(11|7)=$$
$$-(4|7)=-1\ .$$

24. Geometrical proof of (15). Eisenstein gave a simple geometrical interpretation of M in (10) when $p=2\pi+1$ and $q=2Q+1$ are any relatively prime, odd integers and $q<p$.

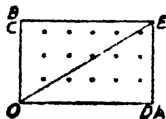


FIG. 1

On square ruled paper let OA, OD, OB, and OC contain $\frac{1}{2}p$, π, $\frac{1}{2}q$, and Q units of length, respectively. Figure 1 is drawn with $p=11$, $q=7$. Take OA as the x-axis and OB as the y-axis. If x and y are integers, the point (x, y) is called a *lattice point*. Since the equation of the diagonal OE is $y=(q/p)x$, a vertical line $x=c$ intersects OE at the point $(c, qc/p)$. Hence if c is a positive integer, $[cq/p]$ is the

number of lattice points on this vertical which lie above the x-axis and on or below OE. There is no lattice point within the segment OE since q/p is in its lowest terms. Hence M *is the number of lattice points which lie inside the triangle* OAE.

Similarly, N in (14) is the number of lattice points which lie inside the triangle OBE. The number of lattice points inside the rectangle $OAEB$ is evidently $Q\pi$. This proves (15).

25. Jacobi's symbol. Let P be a positive odd number. Either $P=1$ or $P=p_1p_2 \cdots p_r$, where $p_1, \ldots, p_r$ are odd primes not necessarily distinct. Then if n is any integer prime to P, we make the definitions

$$(18) \qquad (n|1)=1 \ , \quad (n|P)=(n|p_1) \cdots (n|p_r) \ .$$

If n is a quadratic residue of P and hence of $p_1, \ldots, p_r$, each factor on the right in (18) is $+1$, whence $(n|P)=+1$. But the latter does not imply, conversely, that n is a quadratic residue of P, since an even number $\geqq 2$ of the factors in (18) may be -1. Although Jacobi's symbol has this defect, it is of great importance in theory and in computations.

THEOREM 35. *If n is relatively prime to the positive, odd integers P and Q, then*

$$(19) \qquad (n|P)(n|Q)=(n|PQ) \ .$$

For, if $Q=q_1 \cdots q_s$, where the q's are primes,

$$\begin{aligned}(n|PQ) &= (n|p_1) \cdots (n|p_r)(n|q_1) \cdots (n|q_s) \\ &= (n|P)(n|Q) \ .\end{aligned}$$

THEOREM 36. *If m and n are prime to the positive, odd integer P, then*

$$(20) \qquad (m|P)(n|P)=(mn|P) \ .$$

For, the product of (18) and

$$(m|P)=(m|p_1)\ .\ .\ .\ (m|p_r)$$

is equal, by (2), to

$$(mn|p_1)\cdots(mn|p_r)=(mn|P)\ .$$

THEOREM 37. *When n is prime to the odd $P>0$,*

(21) $$(n|P)=(m|P)\ if\ n\equiv m\ (mod\ P)\ .$$

For, then $n\equiv m \pmod{p_i}$ and $(n|p_i)=(m|p_i)$ by (17) whence

$$(n|P)=\Pi(n|p_i)=\Pi(m|p_i)=(m|P)\ .$$

THEOREM 38. *If P is any positive, odd integer,*

(22) $$(-1|P)=(-1)^{\frac{1}{2}(P-1)}\ ,\quad (2|P)=(-1)^{(P^2-1)/8}\ .$$

Since the product of two even integers is divisible by 4,

(23) $$\begin{cases} P=\Pi\{1+(p_i-1)\}\equiv 1+\Sigma(p_i-1) & \pmod 4\ ,\\ \frac{1}{2}(P-1)\equiv\sum_{i=1}^{r}\frac{1}{2}(p_i-1)=s & \pmod 2\ ,\\ (-1|P)=\Pi(-1|p_i)=(-1)^s=(-1)^{\frac{1}{2}(P-1)}\ . \end{cases}$$

Similarly, since p_i^2-1 is divisible by 8,

$$P^2=\Pi\{1+(p_i^2-1)\}\equiv 1+\Sigma(p_i^2-1)\pmod{64}\ ,$$

$$\pi=\tfrac{1}{8}(P^2-1)\equiv\sum_{i=1}^{r}\tfrac{1}{8}(p_i^2-1)=\sigma\pmod 8\ ,$$

$$(2|P)=\Pi(2|p_i)=(-1)^\sigma=(-1)^\pi\ .$$

THEOREM 39. *If P and Q are positive, odd, relatively prime integers, then*

(24) $$(P|Q)(Q|P)=(-1)^e,\quad e=\tfrac{1}{2}(P-1)\cdot\tfrac{1}{2}(Q-1)\ .$$

For, by (18) and (20),

$$(P|Q)=(P|q_1)\ \ldots\ (P|q_s)=\Pi(p_i|q_j)\ ,$$

where the product is taken for $i=1,\cdots,r$ and $j=1,\cdots,s$. Likewise, $(Q|P)=\Pi(q_j|p_i)$. Hence, by (13) and (23)

$$(P|Q)(Q|P)=\Pi(p_i|q_j)(q_j|p_i)=(-1)^k\ ,$$

$$k=\sum_{i=1}^{r}\sum_{j=1}^{s}\left(\frac{p_i-1}{2}\right)\left(\frac{q_j-1}{2}\right)=\sum_{i=1}^{r}\frac{p_i-1}{2}\cdot\sum_{j=1}^{s}\frac{q_j-1}{2}$$

$$\equiv\tfrac{1}{2}(P-1)\cdot\tfrac{1}{2}(Q-1)=e\pmod 2\ .$$

The generalized reciprocity Theorem 39 simplifies computations. For the example at the end of § 23,

$$(-22|73)=(51|73)=(73|51)=(22|51)=-(11|51)=(51|11)=(-4|11)=(-1|11)=-1\ .$$

EXERCISES IX

1. $(3|73)=1$, $(17|73)=-1$.

2. $(195|1{,}901)=-1$, $(74|101)=-1$, $(365|1{,}847)=1$.

3. $(6|P)=1$ if $P\equiv\pm1$ or $\pm5 \pmod{24}$, -1 if $P\equiv\pm7$ or $\pm11 \pmod{24}$.

4. For P and Q as in Theorem 39, and $2P>Q$,

$$(\pm P|Q)=(-1)^{\frac{1}{2}(P-1)}(\pm P|2P-Q)$$

5. When P is odd and prime to n, write $(n|-P)=(n|P)$. Then (19), (20), (21), and (22_2) hold when P or Q is negative, while (22_1) fails if $P<0$. Also, (24) holds if and only if at least one of the relatively prime, odd numbers P and Q is positive.

6. Let c be a quadratic residue of the prime p, so that $x^2\equiv c \pmod p$ is solvable. If $p=4n+3$, $x\equiv\pm c^{n+1}$. Next, let $p=8n+5$; either $c^{2n+1}\equiv1$, $x\equiv\pm c^{n+1}$, or $c^{2n+1}\equiv-1$, $x\equiv\pm(4n+2)!c^{n+1}$, and $x\equiv\pm\frac{1}{2}(4c)^{n+1}$. Finally, let $p=16n+9$. Either $c^{2n+1}\equiv1$, $x\equiv\pm c^{n+1}$; or $c^{2n+1}\equiv-1$, $x\equiv\pm c^{n+1}N^2$, where N is the $(2n+1)$th power of any non-residue of p, whence $N^4\equiv-1$; or $c^{4n+2}\equiv-1$, $x\equiv\pm ABC$,

where $A=4(2n+1)$, $B=N(N^2-1)$, $C=c^{n+1}(c^{2n+1}-1)$, whence $B^2\equiv 2$, $C^2\equiv 2c$, $2A\equiv -1$.

7. If p is a prime $\equiv 3 \pmod 4$ and if m of the quadratic non-residues of p are $<\frac{1}{2}p$, then

$$1\cdot 2\cdot 3\cdots \tfrac{1}{2}(p-1)\equiv(-1)^m \pmod p .$$

Hint: Use Wilson's theorem. Note that -1 is a non-residue.

8. In Ex. 7 show that m of the quadratic residues are $>\frac{1}{2}p$.

9. Show by induction on n that any quadratic residue of an odd prime p is a quadratic residue of p^n.

CHAPTER IV

INTRODUCTION TO DIOPHANTINE EQUATIONS

26. Historical note. Diophantus, of the third century, proposed many indeterminate problems in his arithmetic. For example, he required that certain combinations of the sides, area, and perimeter of a right triangle shall be rational squares or cubes. He was content with a single numerical, rational solution, although his problems usually have infinitely many rational solutions, and often integral solutions. Much earlier, Pythagoras knew how to find right triangles whose sides can be expressed by integers, i.e., to find integral solutions of

$$(1) \qquad x^2+y^2=z^2 .$$

But it is not more difficult to solve the generalization (2).

27. All integral solutions of

$$(2) \qquad Ax^2+y^2=z^2 \quad (A \text{ with no square factor } >1) .$$

If a prime p divides y and z, then p^2 divides Ax^2, but not A, whence p divides x. Removing the factor p^2 from (2) and proceeding as before, we conclude that the g.c.d. ρ of y and z divides x. Denote the respective quotients by Y, Z, X. Hence

$$(3) \qquad AX^2+Y^2=Z^2 \quad (Y \text{ prime to } Z) ,$$

$$(4) \qquad (Z+Y)(Z-Y)=AX^2 .$$

The g.c.d. of $Z+Y$ and $Z-Y$ divides their sum $2Z$ and difference $2Y$ and hence divides 2. According as the g.c.d. is 2 or 1, we have case I or II.

I. Let $u=\frac{1}{2}(Z+Y)$ and $v=\frac{1}{2}(Z-Y)$ be integers whose g.c.d. is 1. By (4), X is even, say $X=2w$, and $uv=Aw^2$.

Let m^2 and n^2 denote the largest squares which divide u and v, respectively. If p is a prime factor of m, then p^2 divides Aw^2, but not A, whence p divides w. We see in this manner that w is divisible by the relatively prime numbers m and n and hence by their product. Write $w=mnq$. Since the quotients $\alpha=u/m^2$ and $\beta=v/n^2$ are relatively prime, are without square factors >1, and have the product Aq^2, we see that $q^2=1$. Hence

$$(5)\qquad x=2\rho mn,\quad y=\rho(\alpha m^2-\beta n^2),\quad z=\rho(\alpha m^2+\beta n^2)\ ,$$

or $x=-2\rho mn$. The latter case reduces to (5) if we change the signs of ρ, α, β. The solutions are (5) with $\alpha\beta=A$, m and n relatively prime, positive integers, and ρ any integer.

II. Let $Z+Y$ and $Z-Y$ be relatively prime. Hence they are odd and (4) excludes this case if A is even. But if A is odd, we find as in I that

$$(6)\qquad x=\rho mn,\quad y=\tfrac{1}{2}\rho(\alpha m^2-\beta n^2),\quad z=\tfrac{1}{2}\rho(\alpha m^2+\beta n^2)\ ,$$

where $\alpha\beta=A$, m and n are positive, odd, and relatively prime. Since α and β are odd, the numbers (6) are integers.

Let A be odd. If m and n are both odd in (5), then x, y, z are all divisible by 2ρ, whereas ρ is their g.c.d. Hence in (5), one of m and n is even and the other is odd. Evidently (5) is derived from (6) by replacing ρ by 2ρ and using the new values of m, n.

THEOREM 40. *If A is even, all integral solutions of* (2) *are given by* (5). *If A is odd, they are given by* (6), *where ρ is any integer when m and n are odd, but ρ is even when one of m and n is even and the other is odd. In all cases, $\alpha\beta=A$, and m, n are positive and relatively prime.*

From one standpoint it is better not to unite (5) with (6) when A is odd. In (6), m and n were odd; if we replace m by $n+2t$, we obtain x, y, z expressed as polynomials in the integral parameters ρ, n, t, having integral coefficients. The resulting formulas, as well as (5), are called *integral*

formulas since they involve only integers. We then reach the goal of complete solution by integral formulas.

EXERCISES X

1. In (1), x and y are not both odd. All relatively prime, positive, integral solutions with x even are

$$x=2mn, \quad y=m^2-n^2, \quad z=m^2+n^2 \qquad (m>n),$$

where m and n are positive, relatively prime, and one of them is even. Such solutions were known to Diophantus.

2. All relatively prime, positive, integral solutions of $x^2+y^2=z^4$ are $x=4ab(a^2-b^2)$, $y=\pm(a^4+b^4-6a^2b^2)$, $z=a^2+b^2$, or the same with x and y interchanged, where a and b are positive, relatively prime, and one of them is even.

3. All positive, integral solutions, relatively prime in pairs, of $(2x)^4+y^2=z^2$ are $x=ab$, $y=\pm(4a^4-b^4)$, $z=4a^4+b^4$, where a and b are relatively prime, positive integers and b is odd.

4. Solve $c^2AX^2+y^2=z^2$, where A has no square factor. This becomes (2) for $x=cX$. By considering the g.c.d. of c with ρ, m, n in turn, find the cases of (6) when x is divisible by c. Similarly for (5).

28. Equations having no integral solutions.

THEOREM 41. *$x^4+y^4=z^2$ is impossible in integers >0.*

If the theorem is false, there is a least positive integer z for which $z^2=x^4+y^4$, $x>0$, $y>0$. Let d denote the g.c.d. of x and y. Then d^4 divides z^2, and $(z/d^2)^2=(x/d)^4+(y/d)^4$. Hence $z/d^2 \geqq z$, $d=1$. If x and y are both odd, $x^4+y^4\equiv 2 \not\equiv z^2$ (mod 4). Hence one of x and y is even and the other is odd. In view of symmetry, we may take x even and y odd. By Ex. X, 1,

$$x^2=2mn, \quad y^2=m^2-n^2, \quad z=m^2+n^2,$$

where m and n are positive, relatively prime, and one of them is even. If n were odd and hence m even, then $y^2\equiv -1$ (mod 4), which is impossible. Hence

$$n=2q, \quad (\tfrac{1}{2}x)^2=mq, \quad m=r^2, \quad q=s^2,$$

where r and s are relatively prime, positive integers and r is odd. Then $(2s^2)^2+y^2=r^4$, where $2s^2$ and y are relatively prime. As before, $2s^2=2MN$, $r^2=M^2+N^2$, where M and N are relatively prime, positive integers. Thus $M=a^2$, $N=b^2$, $a^4+b^4=r^2$. Since $r \leqq r^2=m \leqq m^2<z$, this contradicts the assumption that z is a minimum.

The theorem proves the case $n=4$ of Fermat's "last theorem" that $x^n+y^n=z^n$ is impossible in integers >0.

EXERCISES XI

1. $x^4+4y^4=z^2$ is impossible in integers >0.

2. $x^4+2y^4=z^2$ is impossible in integers >0. First prove by (5) that all integral solutions of $2X^2+Y^2=Z^2$, with X and Y relatively prime and $X>0$, $Z>0$, are

$$X=2mn, \qquad Y=\pm(m^2-2n^2), \qquad Z=m^2+2n^2,$$

where m and n are relatively prime, positive integers.

3. $x^4-y^4=z^2$ is impossible in integers >0. Hint:

$$z^4+4(xy)^4=(x^4+y^4)^2.$$

4. By the method of Ex. 3, show that each of $x^4-y^4=2z^2$, $x^4-4y^4=\pm z^2$, $8x^4-y^4=\pm z^2$ is impossible in integers >0, while $x^4+y^4=2z^2$ has only the trivial solutions $\pm z=x^2=y^2$.

5. Solve $u^2+py^2=v^2+pw^2$, where p is 1 or an odd prime. Hints: Choose the signs in

$$a=u\pm v, \qquad b=u\mp v, \qquad c=w+y, \qquad d=w-y$$

so that a is divisible by p. To solve $ab=pcd$, write $a=pa'$ and let G denote the g.c.d. of $a'=GA$ and $c=GC$. Then A is prime to C, and $b=CB$, $d=AB$. Hence

$$u=\tfrac{1}{2}(pGA+BC), \qquad \pm v=\tfrac{1}{2}(pGA-BC),$$
$$w=\tfrac{1}{2}(GC+AB), \qquad y=\tfrac{1}{2}(GC-AB)$$

Show that either A, B, C, G are all odd or B and G are even.

6. Solve $x^2+xy+y^2=z^2+zw+w^2$. Hints: Write $u=2x+y$, $v=2z+w$. Apply Ex. 5 with $p=3$. Here $u\equiv y \pmod 2$, whence $(B-G)(A+C)\equiv 0 \pmod 4$. Either A, B, C, G are all odd, or

$B=2\beta$, $G=2g$, and one of $\beta-g$ and $A+C$ is even. Exhibit the values of x, y, $\pm z$, w.

7. Solve $x^2-y^2=z^3$. If $u=x+y$, $v=x-y$, then $u=L^2Mr^3$, $v=LM^2s^3$, $z=LMrs$, where $LM(r-s)$ is even.

29. To find all rational solutions.

THEOREM 42. *If a, b, c, e are integers such that $e\neq 0$ and $d=b^2-4ac$ is not the square of an integer, and if ξ, η, ζ are given rational solutions, not all zero, of*

$$ax^2+bxy+cy^2=ez^2\,, \tag{7}$$

then all its rational solutions are

$$x=\rho r\,,\quad y=\rho s\,,\quad z=\rho t\,, \tag{8}$$

$$\begin{cases} r=-(a\xi+b\eta)u^2-2c\eta uv+c\xi v^2\,,\\ s=a\eta u^2-2a\xi uv-(b\xi+c\eta)v^2\,,\\ t=\zeta T,\quad T=au^2+buv+cv^2\,,\end{cases} \tag{9}$$

where u and v are relatively prime integers, and ρ is rational.

If $z=0$, then $x=y=0$ by the assumption on d, and this solution is of the form (8) with $\rho=0$. Similarly, $\zeta=0$ would imply $\xi=\eta=0$, which is contrary to hypothesis. Thus $\zeta\neq 0$. Henceforth, let $z\neq 0$ and write $X=x/z$, $Y=y/z$. Then (7) becomes

$$aX^2+bXY+cY^2=e\,. \tag{10}$$

This has the rational solution ξ/ζ, η/ζ. The equation of any line through the rational point $(\xi/\zeta, \eta/\zeta)$ is

$$\frac{X-\xi/\zeta}{u}=\frac{Y-\eta/\zeta}{v}\,, \tag{11}$$

where u and v are not both zero. If $u=0$, (11) shall mean $X=\xi/\zeta$. Denote each member of (11) by k. Then

$$X=\frac{\xi}{\zeta}+ku,\qquad Y=\frac{\eta}{\zeta}+kv\,. \tag{12}$$

Substitution of (12) into (10) gives

$$(13) \qquad tk^2+Lk=0\,, \qquad L=2a\xi u+2c\eta v+b(\xi v+\eta u)\,,$$

with t as in (9). Let u and v be rational and not both zero, whence $t\neq 0$. The root $k=0$ yields the known point $(\xi/\zeta,\ \eta/\zeta)$. For the second root $k=-L/t$, (12) become $X=r/t$, $Y=s/t$, where

$$(14) \qquad r=T\xi-Lu\,, \quad s=T\eta-Lv$$

are seen to have the values in (9). We obtain the corresponding solution (8) of (7).

We shall now prove that every rational solution X_1, Y_1 of (10) is expressible in the form r/t, s/t, where r, s, t have the values (9).

First, let the points $(X_1,\ Y_1)$ and $(\xi/\zeta,\ \eta/\zeta)$ be distinct. They determine a line (11) in which $u=X_1-\xi/\zeta$ and $v=Y_1-\eta/\zeta$ are rational and not both zero. Since these two points are the points of intersection of this line and the conic (10), our earlier discussion shows that $X_1=r/t$, $Y_1=s/t$.

Second, let $X_1=\xi/\zeta$, $Y_1=\eta/\zeta$. Then the preceding discussion fails since the line is now indeterminate. Take u and v to be any rational numbers not both zero for which $L=0$. Then (14) give $\xi/\zeta=r/t$, $\eta/\zeta=s/t$. Speaking geometrically, we have replaced the former line by the tangent $L=0$ to (10) at $(\xi/\zeta,\ \eta/\zeta)$.

Hitherto, u and v have been merely rational. We may write $u=NU/D$, $v=NV/D$, where U and V are relatively prime integers, while N and D are integers. Then (9) become the products of the like functions of U and V by N^2/D^2. We take $\rho N^2/D^2$ as a new ρ, and obtain formulas like (8) and (9) in which u and v are now relatively prime integers.

30. To find all integral solutions. Some writers omit the proportionality factor ρ and claim incorrectly that (9) give all integral solutions of (7). Others retain ρ and claim that (7) is solved completely in integers by (8) and (9) without showing how to sort the infinitude of integral solutions from all these rational solutions. This is no less absurd than to ask the reader to start with the algebraic expression for z as a square root of the quotient of the left number of (7) by e.

The following method due to the author is first published here. Let ξ, η, ζ be given integers satisfying (7). For any relatively prime integers u and v, the values r, s, t in (9) are integers. Write $\rho = N/k$, where N and $k>0$ are relatively prime integers. Then x, y, z in (8) are integers if and only if k divides r, s, and t. Let g be the g.c.d. of $k=gD$ and $\zeta = gZ$, whence D is prime to Z. Thus k divides t if and only if D divides T. Then D divides Lu and Lv by (14), and hence divides L itself.

Now L is a linear function $Pu+Qv$ of u and v. Then $L \equiv 0$ or $Pu \equiv -Qv \pmod{D}$ implies $P^2T \equiv Mv^2 \pmod{D}$, where $M = aQ^2 - bPQ + cP^2$. Similarly, $Qv \equiv -Pu$ implies $Q^2T \equiv Mu^2 \pmod{D}$. Since u is prime to v, the facts that T, Mv^2, and Mu^2 are all divisible by D imply that M itself is divisible by D. But

$$(15) \qquad -M = d(a\xi^2 + b\xi\eta + c\eta^2) = de\zeta^2 \, .$$

Hence D divides deg^2.

Thus there is only a finite number of integers D to consider. For a chosen D it is easy to solve the pair of congruences $T \equiv 0$, $L \equiv 0 \pmod{D}$ for u and v. For each set of solutions U, V, the numbers (9) are divisible by D for all integers u and v such that $u \equiv U$, $v \equiv V \pmod{D}$. Replacing u by $U+mD$ and v by $V+nD$, we obtain from r/D, s/D, t/D quadratic functions of m and n with integral coeffi-

cients. It remains to impose the conditions on m and n that these three functions be divisible by g, and hence that r, s, t be divisible by $gD=k$, as desired.

In this way we obtain a finite number of integral formulas which together completely solve (7) in integers.

If $b=2B$, $L=2pu+2qv$, where $p=a\xi+B\eta$, $q=c\eta+B\xi$. Then $2pu\equiv-2qv$ implies $2\eta^2T\equiv 2Ev^2 \pmod{D}$, where $E=aq^2-2Bpq+cp^2$. Since $4E=M$, (15) gives $E=-\Delta c\zeta^2$, where $\Delta=B^2-ac$. Similarly, $2qv\equiv-2pu$ implies $2q^2T\equiv 2Eu^2 \pmod{D}$. Hence D divides $2E$.

THEOREM 43. *All integral solutions of* (7), *having a given solution* ξ, η, ζ *in integers, may be obtained from its rational solutions* (8) *and* (9) *by taking for* ρ *an irreducible fraction whose denominator is* gD, *where* g *divides* ζ, *and* D *divides* L *and* T *and hence also* deg^2. *The last may be replaced by its half*, $2\Delta cg^2$, *when* $b=2B$ $\Delta=B^2-ac$.

31. Example. Let (7) be

$$x^2+y^2=(\xi^2+\eta^2)z^2 . \tag{16}$$

We employ the solution ξ, η, $\zeta=1$. By (9),

$$\begin{cases} r=-\xi u^2-2\eta uv+\xi v^2 , \\ s=\eta u^2-2\xi uv-\eta v^2 , \qquad t=u^2+v^2 . \end{cases} \tag{17}$$

Since $\Delta=-1$, D must divide $2(\xi^2+\eta^2)$.

Consider the case $\xi=1$, $\eta=2$. Then D divides 10. Here

$$r=-u^2-4uv+v^2, \quad s=2u^2-2uv-2v^2, \quad t=u^2+v^2 . \tag{18}$$

If $D=1$, x, y, z are the products of (18) by an arbitrary integer. If $D=2$, the numbers (18) are all even if and only if $u\equiv v \pmod 2$; we obtain integral formulas by replacing u by $v+2w$ and canceling the factor 2 from the expressions derived from (18).

Next, let D be a multiple of 5, whence $D=5\delta$, $\delta=1$ or 2.

In (13), $L=2(u+2v)$. Hence $u+2v$ is divisible by 5. We eliminate $u=5w-2v$ and see that x, y, z are the products of

$$(19) \qquad v^2-5w^2\,, \quad 2v^2-10vw+10w^2\,, \quad v^2-4vw+5w^2$$

by N/δ. These numbers become $-r$, s, t of (18), respectively, when we replace v by $u+2v$ and w by v. This proves

THEOREM 44. *All integral solutions of $x^2+y^2=5z^2$ are the products of $\pm r$, s, t in (18) by integers or by halves of odd integers, provided $u\equiv v$ (mod 2) in the second case.*

EXERCISES XII

1. In the integral formulas obtained in § 31 when $D=2$, replace v by $u+v$ and w by $-v$. We get $-s$, r, t with the values in (18). Hence all integral solutions of $x^2+y^2=5z^2$ are products of $\pm r$, s, t and $\pm s$, r, t by integers.

2. Find all integral solutions of (16) when $\xi=2$, $\eta=3$.

3. Consider (16) when ξ is a prime $\equiv 1$ (mod 4) and $\eta=0$. The cases $D=\xi^2$ and $D=2\xi^2$ are excluded since u is divisible by ξ (by L) and then v is divisible by ξ (by t). Hence D is a divisor of 2ξ and the only condition on u and v is $u\equiv \pm kv$, $k^2\equiv -1$ (mod D).

4. Consider (16) when ξ is a prime $\equiv 3$ (mod 4) and $\eta=0$. The cases in which D is a multiple of ξ are excluded since t is divisible by ξ only when u and v are divisible by ξ.

5. Check the solutions found in Exs. 3 and 4 by means of Ex. X, 1.

6. Solve $x^2+bxy+cy^2=z^2$. Take $\xi=-1$, $\eta=0$, $\zeta=1$. Then

$$r=u^2-cv^2, \qquad s=2uv+bv^2, \qquad t=u^2+buv+cv^2\,.$$

Here D divides b^2-4c, $2u+bv$, and t. If $b=c=1$, either $D=1$, or else $D=3$ and $u\equiv v$ (mod 3) is the only congruential condition.

7. Treat (7) when $d=k^2$, where k is an integer $\neq 0$. Take $2ax+by\pm ky$ as new variables x_1, y_1, whence $x_1y_1=4a\epsilon z^2$. Hence treat (7) with $a=c=0$, $b=1$; its rational solutions are given by (8) and (9). In fact, those of $XY=e$ are obtained from $v=-\eta/\zeta$, $u=X$, since (9) then give $r/t=X$, $s/t=Y$.

8. Find all rational solutions of $aX^2+bY^2+cZ^2=e$, given one solution ξ, η, ζ. Write $X=\xi+ku$, $Y=\eta+kv$, $Z=\zeta+kw$. Then $tk^2+Lk=0$, where

$$t=au^2+bv^2+cw^2, \quad L=2(a\xi u+b\eta v+c\zeta w) .$$

Then $X=r/t$, $Y=s/t$, $Z=l/t$, where $r=t\xi-Lu$, $s=t\eta-Lv$, $l=t\zeta-Lw$. If we attempt to deduce all integral solutions of $ax^2+by^2+cz^2=eW^2$, we meet the difficulty that we cannot eliminate u, v, w from $t\equiv 0$, $L\equiv 0 \pmod D$.

SETS OF INTEGERS HAVING EQUAL SUMS OF LIKE POWERS (§§ 32–35)

32. The numbers 1, 2, and 6 have the same sum and same sum of squares as 4 and 5. We replace the last pair by 0, 4, 5 and obtain sets each involving the same number (three) of integers. In general, the system of m equations

$$(20) \quad x_1^j+\cdots+x_n^j=y_1^j+\cdots+y_n^j \quad (j=1,\ldots,m)$$

is conveniently denoted by the symbol

$$(21) \qquad x_1,\ldots,x_n=y_1,\ldots,y_n \qquad [m] .$$

Hence 1, 2, 6 = 0, 4, 5 [2], and

$$x_1,\ldots,x_n=s-x_1,\ldots,s-x_n \ [2] \qquad \text{if } s=\frac{2}{n}\Sigma x_i .$$

In 1750–51, Goldbach and Euler noted the example

$$(22) \quad a, b, c, a+b+c = 0 , a+b, a+c, b+c \quad [2] .$$

We shall present all known results except numerical examples, and develop new results. Our problem is trivial if $n \leqq m$ in view of

THEOREM 45. *If $n \leqq m$, equations (20) require that $x_1,\ldots,x_n$ form a permutation of $y_1,\ldots,y_n$.*

If $n=m$, we conclude from (20) that each elementary symmetric function of the x's is equal to the same function

of the y's. Hence the equation of degree n having the x's as roots is identical with that having the y's as roots.

If $m>n$, we ignore the values $j=n+1, \ldots, m$. Hence the theorem follows from the preceding case.

The binomial theorem leads at once to

THEOREM 46. *Equations* (21) *imply*

$$(23) \qquad dx_1+a, \ldots, dx_n+a = dy_1+a, \ldots, dy_n+a \quad [m]$$

The former x_i, y_i are here replaced by corresponding terms dx_i+a and dy_i+a of any arithmetical progression.

Conversely, if $d \neq 0$, (23) imply (21).

EXERCISES XIII

1. If $x_1, \ldots, x_n = y_1, \ldots, y_n$ $[m]$, then

$$x_1, \ldots, x_n, y_1+h, \ldots, y_n+h$$
$$= y_1, \ldots, y_n, x_1+h, \ldots, x_n+h \; [m+1] .$$

In case $h=y_i-y_j$, we may delete the equal terms y_j+h and y_i. Similarly, if $h=x_r-x_s$, we may delete x_r and x_s+h.

2. By applying Ex. 1 to a, $b=0$, $a+b$ [1] when $h=c$, we get (22). We now have two cases of a general theorem. Let $x_1, x_2, \ldots$ denote all sums of an odd number of terms chosen from $a_1, \ldots, a_{s+1}$; let $y_1, y_2, \ldots$ denote all sums of an even number of terms chosen from the a's. Then

$$(24) \qquad x_1, \ldots, x_{2^s} = y_1, \ldots, y_{2^s} \quad [s] .$$

Prove by induction on s using Ex. 1 with $h=a_{s+1}$.

3. If $x_1, \ldots, x_n = y_1, \ldots, y_n$ [2], and z is arbitrary, then

$$x_1, \ldots, x_{n-1}, x_n+zy_n, zx_n = y_1, \ldots, y_{n-1}, y_n+zx_n, zy_n \quad [2] .$$

4. If $x_1, \ldots, x_n = y_1, \ldots, y_n$ [2], $a_1, \ldots, a_n = b_1, \ldots, b_n$ [2], and $y_i - x_i = c(b_i - a_i)$ for $i=1, \ldots, n$, then $x_1+a_1, \ldots, x_n+a_n = y_1+b_1, \ldots, y_n+b_n$ [2].

5. The first 2^{s+1} positive integers can be separated into two sets each of 2^s numbers such that (24) hold. For $s=1$, $1+4=$

$2+3$. Proceed by induction from s to $s+1$, applying Ex. 1 with $n=2^s$, $m=s$, $h=2^{s+1}$.

6. If a is odd and >1, the first $4a$ positive integers can be separated into two sets each of $2a$ numbers such that

$$x_1, \ldots, x_{2a}=y_1, \ldots, y_{2a} \quad [2].$$

Proceed by induction from a to $a+2$. Add $4a$ to each term of 1, 4, 6, 7=2, 3, 5, 8 [2], which* was obtained in Ex. 5. Hence

$$1+4a,\ 4+4a,\ 6+4a,\ 7+4a,\ x_1, \ldots, x_{2a}$$
$$=2+4a,\ 3+4a,\ 5+4a,\ 8+4a,\ y_1, \ldots, y_{2a} \quad [2].$$

These two sets together include all integers from 1 to $8+4a=4(a+2)$. The theorem holds when $a=3$ since

$$1, 3, 7, 8, 9, 11=2, 4, 5, 6, 10, 12 \quad [2].$$

7. If a is odd, $a>1$, $s>1$, the first $2^s a$ positive integers can be separated into two sets each of $n=2^{s-1}a$ numbers such that $x_1, \ldots, x_n=y_1, \ldots, y_n$ [s]. This is true by Ex. 6 if $s=2$. Proceed by induction from s to $s+1$, applying Ex. 1 with $m=s$, $h=2^s a$.

8. In Exs. 5 and 7, we may replace the words "positive integers" by successive terms of any arithmetical progression $dz+a$, and replace the formulas by (23) with $m=s$.

9. Arrange 1, . . . , 32 in pairs as follows:

1,8 2,7 3,6 4,5 ; 9,16 10,15 11,14 12,13 ;
17,24 18,23 19,22 20,21 ; 25,32 26,31, 27,30, 28,29 ;

where in each block of four pairs the first numbers ascend and the second descend. Denote each pair by its smaller number. Then

1, 10, 19, 28=4, 9, 18, 27=3, 12, 17, 26=2, 11, 20, 25 [2],
1, 10, 20, 27=4, 9, 19, 26=3, 12, 18, 25=2, 11, 17, 28 [2],
1, 11, 18, 28=4, 10, 17, 27=3, 9, 20, 26=2, 12, 19, 25 [2],
1, 12, 18, 27=4, 11, 17, 26=3, 10, 20, 25=2, 9, 19, 28 [2],
1, 11, 20, 26=4, 10, 19, 25=3, 9, 18, 28=2, 12, 17, 27 [2],
1, 12, 19, 26=4, 11, 18, 25=3, 10, 17, 28=2, 9, 20, 27 [2].

The following quadruples occur distributed among these six:
1, 10, 20, 27=4, 11, 17, 26=3, 12, 18, 25=2, 9, 19, 28 [2].

* It is the only one involving only 1, . . . , 8.

33. Theorem 47. *Every set of integral solutions of*

(25) $$x,\ y,\ z=u,\ v,\ w \quad [2]$$

is obtained by adding an arbitrary integer to each term of

(26) $$AD,\ AG+BD,\ BG=AD+BG,\ BD,\ AG \quad [2]\ .$$

By choice of integers a and b we have $x=u-b$, $y=v+a$. Then $z=w-a+b$. Write $a=GA$, $b=GB$, where A is prime to B. Write $U=u-b$, $W=w-a$. Then $\Sigma x^2=\Sigma u^2$ if $BU=Av+(B-A)W$. We may express U in the form $rA+c$. The last equation is equivalent to $A(v-rB-c)=(A-B)(W-c)$. Since A is prime to $A-B$, this requires

$$v-rB-c=(A-B)Q\ , \quad W-c=AQ\ .$$

Write D for $r-Q$. The values of u, v, w are obtained by adding $c+AQ$ to the numbers in the second member of (26). From $x=u-b$, etc., we get the first member.

EXERCISES XIV

1. The first set of three numbers in (26) form a permutation of the second set if and only if $ABCD=0$, or $A=B$, or $D=G$.

2. If $r(u-x)+s(v-y)+t(w-z)=0$, (25) implies

(27) $$x+r,\ \ y+s,\ \ z+t=u+r,\ \ v+s,\ \ w+t \quad [2]\ ,$$

and conversely. Then (27) is said to be derived from (25).

3. Every integral solution of (25) can be derived from

(28) $$0,\ a,\ b=b,\ 0,\ a\ \ [2]\ ,$$

where $a=y-v$, $b=u-x$, by using $r=x$, $s=v$, $t=w+v-y=z+x-u$. To verify the first equation in Ex. 2, employ the first t and

$$(x-u)^2+x^2-u^2=(v+w-y-z)^2+v^2+w^2-y^2-z^2\ .$$

4. Subtract t from each number in the solution given by Ex. 3. Hence it suffices to add r, s, 0 to the members of (28).

Write $a=GA$, $b=GB$, where A is prime to B. Then $rb-sa=0$ requires $r=AD$, $s=BD$. We get (26) and hence another proof of Theorem 47.

5. By Theorem 46, equations (25) are equivalent to

$$3x-s,\ 3y-s,\ 3z-s=3u-s,\ 3v-s,\ 3w-s\ [2]\ .$$

Take $s=x+y+z$. Hence the solution of (25) reduces to that of

$$(29)\qquad \Sigma X=0,\qquad \Sigma U=0,\qquad \Sigma X^2=\Sigma U^2\ .$$

Elimination of Z and W gives

$$(30)\qquad X^2+XY+Y^2=U^2+UV+V^2\ ,$$

all of whose integral solutions were found in Ex. XI, 6.

6. The two equations

$$(31)\qquad \Sigma X=\Sigma U,\qquad \Sigma X^2=\Sigma U^2$$

imply $\Sigma XY=\Sigma UV$, whose square is

$$(32)\qquad \Sigma X^2Y^2+2XYZ\Sigma X=\Sigma U^2V^2+2UVW\Sigma U\ .$$

From this, the linear equations (29) and the square of the last equation (29), we get

$$(33)\qquad \Sigma X^4=\Sigma U^4\ .$$

Hence (29) imply (33).

7. Consider the system S of three equations (31) and (33). They imply (32) and hence $(XYZ-UVW)\Sigma X=0$. If we exclude the trivial case in which X, Y, Z form a permutation of U, V, W, we have $\Sigma X=0$, and see that S reduces to (29) and hence to (30).

8. If $a+b+c=0$, $n=1, 2, 4$,

$$(ja+kb)^n+(jb+kc)^n+(jc+ka)^n$$
$$=(jb+ka)^n+(jc+kb)^n+(ja+kc)^n\ .$$

9. If $x_1^2, \ldots, x_n^2=y_1^2, \ldots, y_n^2\ [m]$, then

$$x_1,\ -x_1,\ \ldots,\ x_n,\ -x_n=y_1,\ -y_1,\ \ldots,\ y_n,\ -y_n\ [2m+1]\ .$$

Derive cases of this from Exs. 8, 10, 11.

10. The following sets have the same sums of squares and same sums of fourth powers:

$$m^2+mn+3n^2\ ,\quad 2m^2-4mn-n^2\ ,\quad 3m^2-2n^2\ ;$$
$$3m^2-mn+n^2\ ,\quad m^2-4mn-2n^2\ ,\quad 2m^2-3n^2\ .$$

$$ab+aB+bA-3AB\ ,\quad ab-aB-bA-3AB\ ,\quad 2aB+2bA\ ;$$
$$ab+aB-bA+3AB\ ,\quad ab-aB+bA+3AB\ ,\quad 2aB-2bA\ .$$

11. $2^2, 16^2, 21^2, 25^2=5^2, 14^2, 23^2, 24^2$ [3].

12. We obtain (29) from (25) if we write

$$X=y-z\ ,\qquad Y=z-x\ ,\qquad Z=x-y\ ,$$
$$\pm U=v-w\ ,\quad \pm V=w-u\ ,\quad \pm W=u-v\ .$$

In accord with (30), we choose the sign so that $X-Y\equiv\pm(U-V)$ (mod 3). Conversely, a solution of (29) determines only the differences of x, y, z and the differences of u, v, w. To get (25) we need also

$$3z+X-Y=3w\pm(U-V)\ ,$$

which yields an integer z for every assigned w. Hence again, problem (25) reduces essentially to (30).

13. Solve (34) by the method of Ex. 5.

34. Theorem 48. *Every set of integral solutions of*

(34) $$x,\ y,\ z,\ w=\xi,\ \eta,\ \zeta,\ \omega\quad [2]$$

is obtained by adding an arbitrary integer to each term of

$$u+gGb\ ,\quad v\ ,\quad gQ+GC\ ,\quad gG(a+b)$$
$$=u+gG(a+b),\ v+gGb,\ gQ,\ GC\quad [2]\ ,$$

where a is prime to b, g is prime to C, and

(35) $$au+bv=CQ\ .$$

From a particular solution r, s of

(36) $$as+br=1\ ,$$

we get all solutions of (35):

(37) $$u=sCQ+bT\ ,\quad v=rCQ-aT\ .$$

We may take $x=\xi-\alpha$, $y=\eta-\beta$, $z=\zeta+\gamma$, $w=\omega+\alpha+\beta-\gamma$. Write $X=\xi-\alpha-\beta$, $Y=\eta-\beta$, $W=\omega-\gamma$, $\alpha=GA$, $\beta=GB$, $\gamma=GC$, where A, B, C have no common factor >1. Then $\Sigma x^2=\Sigma\xi^2$ if

$$(38) \qquad -AX-BY+C\zeta+(A+B-C)W=0 .$$

Let g denote the g.c.d. of $A=ga$ and $B=gb$. Express X in the form $Rb+c$. Write $L=Y+Ra-c$, $M=\zeta-c$, $N=c-W$. Then (38) becomes $g[bL+(a+b)N]=C(M+N)$. Since g is prime to C, $M+N=gQ$, $b(L+N)+aN=CQ$. Multiply the final number by (36). Thus

$$b(L+N-rCQ)+a(N-sCQ)=0 .$$

Since a is prime to b, the quantities in parentheses are equal to $-at$ and bt, respectively, where t is an integer. Hence

$$N=sCQ+bt\ , \quad L=(r-s)CQ-(a+b)t\ ,$$
$$M=gQ-sCQ-bt\ .$$

Thus ξ, η, ζ, ω are obtained by adding $k=c-bt-sCQ$ to the four numbers in the second member of the long formula in the theorem and writing T for $t+R$. We get the first member from $x=\xi-\alpha$, etc.

35. Methods for finding all integral solutions of

$$(39) \qquad x,\ y,\ z,\ w=\xi,\ \eta,\ \zeta,\ \omega \quad [3] .$$

This system of three equations is equivalent to that composed of the two equations (34) and

$$(40) \qquad \Sigma xyz=\Sigma\xi\eta\zeta .$$

For, if s_j denotes the sum of the jth powers of x, y, z, w, Newton's identities in the theory of equations give

$$6\Sigma xyz=s_1^3-3s_1s_2+2s_3 .$$

I. Employ the solution in Theorem 48 and call it trivial if the four terms of one member form a permutation of those of the other. By Theorem 45 this will be the case if any term of one member is a term of the other and hence if $gG=0$. After deleting the factor gG, we find that (40) reduces to

$$(41)\qquad [u+v+gG(a+2b)]QC=v(u+gGb)(a+b) \\ +(au+bv)(gQ+GC)\ .$$

I_1. Assign integral values to a, b, Q, C and take an integral solution u, v of (35). Then (41) becomes an equation of the form

$$AgG+Bg+DG+E=0$$

in the unknowns g and G. Multiply by A. We get

$$(Ag+D)(AG+B)=BD-AE\ .$$

Express $BD-AE$ in all ways as a product of two factors k and l such that $k\equiv D$, $l\equiv B$ (mod A). Then the solutions are

$$g=\frac{k-D}{A}\ ,\qquad G=\frac{l-B}{A}\ .$$

The excluded case $A=0$ is still simpler.

I_2. Elimination of u between (35) and (41) gives a quadratic in v which, after the square is completed, is

$$b^2[2(a+b)v-2QC-gGa(a+b)]^2=F\ ,$$
$$F=(a+b)^2(g^2G^2a^2b^2-4gGQCab)-4abQ^2C^2 \\ +4QCab(a+b)(gQ+GC)\ .$$

Assign integral values to a, b, g, C. Then F is a homogeneous, quadratic function of G and Q with known, integral coefficients. In § 30, we showed how to find all integers G and Q for which F is a square.* The parameters involved

* F is unaltered when C is replaced by $(a+b)g-C$ and Q by $(a+b)G-Q$, whence one solution yields another

in this solution for G and Q are to be restricted so that the resulting, rational value of v is an integer such that $CQ-bv$ is divisible by a, whence (35) yields an integer u.

II. From the quadruple of each term of (39) subtract $S=x+y+z+w$. By Theorem 46 we obtain an equivalent system (39) in which now $S=0$. Write

$$A=x+y=-z-w\ ,\quad B=\tfrac{1}{2}(x-y+z-w)\ ,$$
$$C=\tfrac{1}{2}(x-y-z+w)\ ,$$

and α, β, γ for the like functions of ξ, η, ζ, ω. Then $A, \ldots, \gamma$ are integers. Conversely, if A, B, C are integers, then

$$2x=A+B+C,\ 2z=B-C-A,\ y=A-x,\ w=-A-z$$

determine values of x, y, z, w which are all integers if only one of A, B, C is even or if all are even. Then $\Sigma x^2=\Sigma\xi^2$ is equivalent to

(42) $$A^2+B^2+C^2=\alpha^2+\beta^2+\gamma^2\ .$$

Using $A=\frac{1}{2}(x+y)-\frac{1}{2}(z+w)$, we find that

$$8ABC=\Sigma x^3-\Sigma x^2y+2\Sigma xyz\ .$$

But when $\Sigma x=0$, Newton's identities give $\Sigma x^3-3\Sigma xyz=0$. Also,

$$0=(\Sigma x)^3=\Sigma x^3+3\Sigma x^2y+6\Sigma xyz\ .$$

Hence $3ABC=\Sigma x^3$, and the cubic equation in (39) may be replaced by

(43) $$ABC=\alpha\beta\gamma\ .$$

By use of the g.c.d. X of A and α, etc., we readily verify that all integral solutions of (43) are of the form

$$A=lpX,\ B=mqY,\ C=nrZ,\ \alpha=mrX,\ \beta=npY,\ \gamma=lqZ\ .$$

For assigned integers l, m, n, p, q, r, (42) is of the form

(44) $$aX^2+cY^2=eZ^2\ ,$$

whose integral solutions can be found by §§ 29, 30. For, it has the particular solution $X=q$, $Y=r$, $Z=p$, since then $A=\gamma$, $B=\alpha$, $C=\beta$. Also the solution $X=n$, $Y=l$, $Z=m$ whence $A=\beta$, $B=\gamma$, $C=\alpha$.

EXERCISES XV

1. If only one or all three of A, B, C are even, the same is true of α, β, γ by (42) and (43).

2. Equations (39) hold if

$$x=(a+b)j+(b+c)k+(c+d)l+(d+a)m\ ,$$

while y is obtained from x, z from y, and w from z by replacing a by b, b by c, c by d, and d by a. Also, ξ, η, ζ, ω are derived from x, y, z, w by interchanging a with d, and b with c.

3. To solve (20) when $m=2$ assign any values to x_i and y_i for $i\geqq 3$. Write $X=\Sigma x_i$, $Y=\Sigma y_i$, $u=\Sigma x_i^2$, $v=\Sigma y_i^2$, where all summations extend from 3 to n. Write $S=x_1+x_2+X$, $f=x_1-x_2$, $g=y_1-y_2$. Then

$$x_1=\tfrac{1}{2}(S-X+f),\qquad x_2=\tfrac{1}{2}(S-X-f),\qquad y_1=\tfrac{1}{2}(S-Y+g),$$
$$y_2=\tfrac{1}{2}(S-Y-g)$$

are integers if f and $S-X$ are of the same parity and likewise and $S-Y$. The quadratic equation becomes

$$f^2-g^2=(S-Y)^2-(S-X)^2+2v-2u\ .$$

Its second member must be expressed as a product of two factors of the same parity. This is always possible by Ex. I, 9, since it is never $\equiv 2 \pmod 4$.

36. All rational solutions of

$$W^3+X^3+Y^3+Z^3=0\ . \tag{45}$$

Write $W=p+q$, $X=p-q$, $Y=r-s$, $Z=-r-s$. We get

$$p(p^2+3q^2)=s(s^2+3r^2)\ . \tag{46}$$

Write $2p=x+w$, $2s=x-w$, $2q=y+z$, $2r=y-z$. Then

$$w^3+3w(x^2+y^2+z^2)+6xyz=0 \tag{47}$$

This may be expressed in determinantal form

$$\begin{vmatrix} w & 3z & -3y \\ -z & w & 3x \\ y & -x & w \end{vmatrix} = 0 .$$

Hence there exist rational solutions a, b, c, not all zero, of

$$wa+3zb-3yc=0 , \quad -za+wb+3xc=0 , \quad ya-xb+wc=0 .$$

Elimination of y and z gives $(a^2+3b^2+3c^2)w+6bcx=0$, if $a\neq 0$, and the solutions are

$$(48) \quad \begin{cases} w=-6\rho abc , & x=\rho a(a^2+3b^2+3c^2) , \\ y=\rho b(a^2+3b^2+9c^2) , & z=3\rho c(a^2+b^2+3c^2) . \end{cases}$$

But if $a=0$, then $(b^2+3c^2)w=0$, $w=0$, $x=0$, and we again have (48).

THEOREM 49. *All rational solutions of (47) are given by (48) for integers a, b, c without a common factor >1 and for ρ rational.*

From them we obtain all rational solutions of (46) and hence of (45).

EXERCISES XVI

1. Euler's rational solution of (46) was simplified by Binet in 1841. If $s\neq 0$ we can find rational solutions a and b of $p=sa+3rb$, $q=-ra+sb$, since the determinant of their coefficients is $s^2+3r^2\neq 0$. Write β for a^2+3b^2. Then $p^2+3q^2=\beta(s^2+3r^2)$ and (46) becomes $(as+3br)\beta=s$. Hence we can choose rational numbers ρ and σ not both zero such that $\sigma s=-3\rho b\beta$, $\sigma r=\rho(a\beta-1)$. If $b\neq 0$ take $\sigma=1$. If $b=0$, whence $a=1$, and r, s are arbitrary, take $\sigma=0$, $\rho=1$. Write $a=A/C$, $b=B/C$, $D=A^2+3B^2$, $\tau=\sigma C^4$. Then

$$\tau s=-3\rho BCD, \quad \tau r=\rho C(AD-C^3), \quad \tau p=-3\rho BC^3, \quad \tau q=\rho(AC^3-D^2) .$$

This solution is of the fourth degree in A, B, C. It does not include all the solutions having $s=0$, whence $p=0$.

2. All rational solutions of

$$x^2y+y^2z+z^2w+w^2x-\begin{vmatrix} z & -x & 0 \\ x & y & -w \\ w & z & y \end{vmatrix}=0$$

are

$$\rho x=-a(ab+c^2)\ ,\quad \rho y=a^3+b^2c\ ,$$
$$\rho z=-b(ab+c^2)\ ,\quad \rho w=b^3-a^2c\ .$$

3. Find all rational points of the surface

$$S\colon\quad f(x,y)=f(w,z),\qquad f(x,y)\equiv Ax^3+Bx^2y+Cxy^2+Dy^3\ .$$

If ω is an imaginary cube root of unity, the lines

$$R.\quad x=\omega w,\ y=\omega z;\qquad r\colon\ x=\omega^2w,\ y=\omega^2z$$

lie on S and are called *rulings*. The line

$$L\colon\quad x=ay+bz\ ,\quad w=cy+dz$$

meets R if and only if $b=-c$, $d=a+c$ Then L meets also r, while L then meets S in the points for which $\alpha y^3+\ldots-\beta z^3=0$, where

$$\alpha=f(a,1)-Ac^3,\quad \beta=f(a+c,1)+Ac^3$$

To discard the points that lie on R and r, we remove from $\alpha y^3+\ldots$ the factor $(y-\omega z)(y-\omega^2z)$ and evidently obtain $\alpha y-\beta z=0$ for the third point in which L meets S. Unless $\alpha=\beta=0$, this point has

$$\rho y=\beta,\quad \rho z=\alpha,\quad \rho x=a\beta-c\alpha,\quad \rho w=c\beta+(a+c)\alpha\ .$$

Inserting the values of α and β, we have the desired rational points expressed in terms of the parameters a, c. Possible additional points are those on rulings of type L (whence $\alpha=\beta=0$), and points on both S and the unique line $y=z=0$ which meets R and r and is not solvable for x and w in terms of y and z.

4. Apply the method of Ex. 3 to Ex. 2 and to (45).

37. Equal sums of two fourth powers. The complete solution of

(49) $$X^4+Y^4=Z^4+W^4$$

in integers has not yet been found. Euler took

(50) $$X=p+q,\ W=p-q,\ Z=r+s,\ Y=r-s$$

and noted that (49) becomes

(51) $$pq(p^2+q^2)=rs(r^2+s^2)\ .$$

It is not more difficult to treat the generalization

(52) $$pq(mp^2+nq^2)=rs(mr^2+ns^2)\ .$$

Define rational numbers a, b, w by $q=ra$, $s=pb$, $a=bw$. From (52) we get

(53) $$\frac{p^2}{r^2}=\frac{nb^2w^3-m}{nb^2-mw}=\frac{\alpha w^3-\beta}{\alpha-\beta w}\ ,$$

after dividing numerator and denominator by nb^2-m and writing $\alpha=nb^2/(nb^2-m)$, $\beta=\alpha-1=m/(nb^2-m)$. We shall have a rational value of p/r if we choose w so that $(\alpha w^3-\beta)(\alpha-\beta w)$ is a rational square. This problem to make a quartic function of w a square arises in many Diophantine questions, but has not been completely solved. Euler here employed a special device. For $w=z+1$, the final fraction in (53) becomes

$$\frac{\alpha z^3+3\alpha z^2+3\alpha z+1}{1-\beta z}\ .$$

Equate this to $(1+dz)^2$ and cancel a factor z. We get

$$(\alpha+\beta d^2)z^2+Az+B=0\ , \qquad A=3\alpha+2\beta d-d^2\ ,$$
$$B=3\alpha+\beta-2d\ .$$

Choose d so that $B=0$. Since $\beta=\alpha-1$, we see that $4A=3$. Hence $z=-3/(4\alpha+4\beta d^2)$. Having w, we obtain rational solutions of (52) with r and b arbitrary.

To return to (51), take $m=n=1$. Write $b=f/g$. We now express α, β, d, z, and $p/r=1+dz$ in terms of f and g. Discarding the factor of proportionality, we obtain

THEOREM 50. *Equation* (51) *has the solutions*

$$p=g(f^2+g^2)(-f^4+18f^2g^2-g^4) \,,$$
$$r=2g(4f^6+f^4g^2+10f^2g^4+g^6) \,,$$
$$q=2f(f^6+10f^4g^2+f^2g^4+4g^6) \,,$$
$$s=f(f^2+g^2)(-f^4+18f^2g^2-g^4) \,.$$

EXERCISES XVII

1. For $f=1$, $g=3$, the values of p, q, r, s are the products of 75, 193, 291, 25 by 32. Discarding the factor 2 from $X, \ldots, W$, we get

$$(54) \qquad 134^4+133^4=158^4+59^4 \,,$$

which is said to be the solution in least integers.

2. One solution of (51) yields another solution

$$p'=p+q+r+s,\ q'=p+q-r-s,\ r'=p-q+r-s,\ s'=p-q-r+s \,.$$

But they yield numbers proportional to (50).

3. For $F(X,\ W)=k(X^4-W^4)+2lXW(X^2-W^2)$, the solution of $F(X,W)=F(Z,Y)$ reduces to (52). Hence infinitely many solutions are known.

4. Equation (51) has the solution

$$p=t\phi(t,h),\ q=3t^2h^6,\ r=h\phi(h,t),\ s=3t^6h^2 \,,$$

where $\phi(t,h)=t^6+t^4h^2-2t^2h^4+h^6$. For $t=2$, $h=1$, this gives (54).

5. For integers, (50) holds if either X or Y is congruent modulo 2 to either Z or W. In the contrary case, (49) fails modulo 4.

CHAPTER V

BINARY QUADRATIC FORMS

The problem to find all integral solutions of $x^2+y^2=41$ is equivalent to that for $X^2+4XY+5Y^2=41$, which is derived from the first equation by the transformation $x=X+2Y$, $y=Y$. Similarly, there are infinitely many equations equivalent to the first one. It would be mere duplication of work to solve more than one of them. It is now clear why we study transformations and equivalence. The theory applies to all real forms, except when the form is explicitly called integral (i.e., has integral coefficients).

38. Transformation. If a, b, c are constants and x and y are independent variables, the function

(1) $$q=ax^2+bxy+cy^2$$

is called a *binary quadratic form*. The particular letters used to denote the variables are usually immaterial. Thus (1) is determined by its coefficients and is denoted by (a, b, c). Its *discriminant* is

(2) $$d=b^2-4ac\ .$$

Consider a linear transformation

(3) $$\tau:\ x=\alpha X+\beta Y\ ,\quad y=\gamma X+\delta Y\ ,\quad \Delta=\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix}\neq 0\ ,$$

of determinant Δ. If we insert these expressions for x and y into (1), we get another form

(4) $$Q=AX^2+BXY+CY^2$$

having the coefficients

(5) $$A=a\alpha^2+b\alpha\gamma+c\gamma^2\ ,\quad C=a\beta^2+b\beta\delta+c\delta^2\ ,$$

(6) $$B=2a\alpha\beta+b(\alpha\delta+\beta\gamma)+2c\gamma\delta\ .$$

Transformation (3) is said to *replace* q by Q, or *transform* q into Q. The discriminant of Q is

$$(7)\qquad \begin{vmatrix} B & 2C \\ 2A & B \end{vmatrix} = \begin{vmatrix} \delta & \beta \\ \gamma & \alpha \end{vmatrix} \cdot \begin{vmatrix} b & 2c \\ 2a & b \end{vmatrix} \cdot \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} = \Delta^2 d \,.$$

To Q we apply the new transformation

$$(8)\qquad t:\ X = r\xi + s\eta\,,\quad Y = g\xi + h\eta\,,\quad D = \begin{vmatrix} r & s \\ g & h \end{vmatrix} \neq 0\,,$$

and obtain a form f in the variables ξ and η. By eliminating X and Y between equations (3) and (8), we obtain

$$(9)\qquad x = k\xi + l\eta\,,\qquad y = m\xi + n\eta\,,$$

$$(10)\qquad k = \alpha r + \beta g\,,\ l = \alpha s + \beta h\,,\ m = \gamma r + \delta g\,,\ n = \gamma s + \delta h\,.$$

Then

$$(11)\qquad \begin{vmatrix} k & l \\ m & n \end{vmatrix} = \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} \cdot \begin{vmatrix} r & s \\ g & h \end{vmatrix} = \Delta D\,.$$

Hence (9) is a transformation of determinant $\Delta D \neq 0$ which replaces q by f. This transformation (9) has the same effect upon q as the successive applications of transformations (3) and (8), and is called the *product* of the latter, taken in the order indicated, and denoted by τt.

A transformation is determined by its coefficients. We may denote transformations (3), (8), and (9) by their *matrices*, as exhibited in

$$(12)\qquad \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \cdot \begin{pmatrix} r & s \\ g & h \end{pmatrix} = \begin{pmatrix} k & l \\ m & n \end{pmatrix}.$$

Formulas (10) lead to a simple rule to find the product of two matrices. For example, the element m in the second row and first column of the product is obtained by multiplying the elements γ, δ in the second row of the first matrix by the corresponding elements r, g in the first column

of the second matrix and adding these products. Briefly multiply row of the first by column of the second. As in (11), this is one of the permissible methods for multiplying determinants.

We readily prove the associative law $\tau t \cdot T = \tau \cdot tT$ whence each product may be denoted by τtT. Let

$$(13) \qquad T: \quad \xi = \lambda u + \mu v \,, \qquad \eta = \rho u + \sigma v \,.$$

Since tT is obtained by eliminating ξ, η between (8) and (13), $\tau \cdot tT$ is obtained from (3), (8), (13) by eliminating first ξ and η and then X and Y, to obtain x and y as functions of u and v. We evidently obtain the same result if we eliminate first X and Y and then ξ and η, which yields $\tau t \cdot T$.

39. Equivalent forms. Henceforth we employ only *integral*, linear transformations having integral coefficients of determinant ± 1. Solving the equations (3) of such a transformation, we get

$$(14) \qquad X = \pm \delta x \mp \beta y \,, \qquad Y = \mp \gamma x \pm \alpha y \,.$$

To secure notations in agreement with (8), we replace x, y by ξ, η in (14) and get the transformation

$$(15) \qquad X = \pm \delta \xi \mp \beta \eta \,, \quad Y = \mp \gamma \xi \pm \alpha \eta \,.$$

The product of (3) by (15) is the *identity* transformation

$$(16) \qquad x = \xi \,, \qquad y = \eta \,.$$

Hence (15) is called the *inverse* of transformation τ in (3) and is denoted by τ^{-1}. Since $q = Q$ in view of relations (3) or the equivalent relations (14), we see that if transformation τ replaces q by Q, the inverse transformation τ^{-1} replaces Q by q.

According as the determinant $\alpha\delta - \beta\gamma$ of (3) is $+1$ or -1, q is said to be *(properly) equivalent* or *improperly*

equivalent to Q. Since the determinant of (15) is also $\alpha\delta-\beta\gamma$, then Q is equivalent or improperly equivalent to q, respectively. By (7), properly or improperly equivalent forms have the same discriminant. When q and Q are equivalent we write $q \backsim Q$.

For example, $q=2x^2+3y^2$ is equivalent to $Q=3X^2+2Y^2$ under the transformation $x=Y$, $y=-X$, of determinant 1. The inverse transformation is $X=-\eta$, $Y=\xi$, which replaces Q by $2\xi^2+3\eta^2$. Hence $q \backsim Q$.

If $q \backsim Q$ and $Q \backsim f$, then $q \backsim f$ by § 38. Hence all forms equivalent to a given form Q are equivalent to each other and are said to form a *class*.

A form Q is said to *represent* the number m if there exist integers X and Y such that $Q=m$. Then x and y in (3) are integers, so that q represents m. In case $\alpha\delta-\beta\gamma=\pm 1$, the converse is true by (14). Hence *equivalent forms represent the same integers.*

EXERCISES XVIII

1. If $\tau=\begin{pmatrix} 3 & 2 \\ -1 & -1 \end{pmatrix}$, $t=\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, then $\tau t=\begin{pmatrix} 5 & 2 \\ -2 & -1 \end{pmatrix}$, $t\tau=\begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}$.

2. If also $T=\begin{pmatrix} 2 & -2 \\ 2 & 2 \end{pmatrix}$, verify that $\tau t \cdot T=\tau \cdot tT$.

3. $(\tau t \cdot T)T'=\tau(t \cdot TT')=\tau t \cdot TT'$.

4. Every form is equivalent to itself.

5. ax^2+cy^2 is improperly equivalent to itself.

6. Two *opposite* forms $[a, b, c]$, $[a, -b, c]$ are improperly equivalent.

7. $[a, b, c]$ and $[a, b', c']$ are called *parallel* forms if they have the same discriminant and if $b'=b+2a\beta$, where β is an integer. They are equivalent and the first becomes the second when x is replaced by $x+\beta y$. The discriminants are equal if and only if $c'=c+b\beta+a\beta^2$.

8. $[a, b, c]$ is equivalent to $[c, -b, a]$ and improperly equivalent to $[c, b, a]$.

9. x^2+y^2 represents 1, 2, 4, 5, and 41.

40. Definite and reduced forms. Let the discriminant d of (1) be negative. Write $d=-\Delta$. Then

$$4aq=(2ax+by)^2+\Delta y^2\ , \quad \Delta>0\ . \tag{17}$$

Let a, b, c be real. If $a>0$, q is positive for all real numbers x and y not both zero, and q is then called a *positive* form. If $a<0$, q takes only negative and zero values and is called a *negative* form; then $-q$ is a positive form. Negative forms may be ignored since their properties follow at once from those of positive forms. Both positive and negative forms are called *definite*. But if $d>0$, then $\Delta<0$ and q in (17) evidently takes both positive and negative values and is called *indefinite;* such forms are treated in chapter vii.

Let q be a real, positive form. If p is positive, the condition $q\leqq p$ is equivalent by (17) to

$$(2ax+by)^2+\Delta y^2\leqq 4ap\ .$$

This requires that $y^2\leqq 4ap/\Delta$, which holds for only a limited number of integers y. To each such y correspond a limited number of integers x such that the inequality holds. Hence $q\leqq p$ holds for only a finite number of pairs of integers x, y. In other words, q represents only a finite number of numbers $\leqq p$. Choose p to be the number a represented by q when $x=1$, $y=0$. Hence there is a minimum $A>0$ of all numbers represented by q. Moreover, we can find, in a finite number of steps, integers $x=\alpha$, $y=\gamma$ for which q takes its minimum A.

These integers α, γ have no common divisor $D>1$ since $q=A/D^2$ when $x=\alpha/D$, $y=\gamma/D$. Hence there exist integers β and δ such that $\alpha\delta-\gamma\beta=1$. Then transformation (3) has determinant 1 and replaces q by an equivalent form

$Q=[A, l, m]$ in the variables X, Y. The transformation $X=\xi+n\eta$, $Y=\eta$ has determinant 1 and replaces Q by $F=[A, B, C]$, where $B=l+2nA$. We can choose an integer n so that $-A<B\leqq A$. Since C is the value of F for $\xi=0$, $\eta=1$, it is represented by the equivalent form q. Hence C is not less than the minimum A of q. In case $C=A$, the transformation $\xi=-y$, $\eta=x$ has determinant 1 and replaces F by $[A, -B, A]$.

A positive form $[a, b, c]$ is called *reduced* if

$$-a<b\leqq a\ ,\quad c\geqq a\ ,\ \text{with}\ b\geqq 0\ \text{if}\ c=a\ . \tag{18}$$

THEOREM 51. *Every real, positive form q is equivalent to a reduced form.*

A positive form $[a, b, c]$ is called *semi-reduced* if

$$c\geqq a\geqq |b|\ . \tag{19}$$

If its discriminant is $-\Delta$, then

$$4a^2\leqq 4ac=\Delta+b^2\leqq\Delta+a^2\ ,\quad 3a^2\leqq\Delta\ ,$$

$$a\leqq\sqrt{\tfrac{1}{3}\Delta}\ . \tag{20}$$

Any reduced form is semi-reduced, but not conversely.

Our discussion leads to an integral transformation of determinant unity which replaces q by a reduced form.

For example, let $q=5x^2-4xy+2y^2$. If 2 were not the minimum of q, there would be integral solutions of

$$q=2(y-x)^2+3x^2=1\ .$$

We may take $\alpha=0$, $\gamma=1$, $\delta=0$, $\beta=-1$. Here (3) is $x=-Y$, $y=X$, which replaces q by $Q=2X^2+4XY+5Y^2$. The transformation $X=\xi-\eta$, $Y=\eta$ replaces Q by $F=2\xi^2+3\eta^2$, which is reduced The product $x=-\eta$, $y=\xi-\eta$ of these two transformations replaces q by F.

41. Neighboring forms. The transformation

$$\begin{pmatrix} 0 & 1 \\ -1 & \delta \end{pmatrix} \tag{21}$$

has determinant unity and replaces $q=[a, b, a_1]$ by the equivalent form $Q=[a_1, b_1, a_2]$, in which

$$b_1=-b-2\delta a_1 , \quad a_2=a+b\delta+a_1\delta^2 . \tag{22}$$

We call Q a *right neighboring form* to q, and call q a *left neighboring form* to Q. The sum of their middle coefficients is the product of their common coefficient a_1 by an even integer -2δ, while their discriminants are equal. Conversely, any two such forms are neighboring, since (21) replaces q by $[a_1, b_1, c]$, whose discriminant is equal to that of Q, whence $c=a_2$.

For the case of integral forms q (i.e., having integral coefficients), Gauss proved Theorem 51 as follows Among the right neighboring forms Q to q there occurs one in which $a_1 \geqq |b_1|$. For, we may divide $-b$ by $2a_1$ and obtain an integral quotient δ and an integral remainder r such that $|r| \leqq a_1$. Then by (22),

$$-b=2a_1\delta+r , \quad b_1=r , \quad |b_1| \leqq a_1 .$$

Then if also $a_2 \geqq a_1$, Q is semi-reduced. But if $a_2 < a_1$, we transform Q into a right neighboring form $h=[a_2, b_2, a_3]$ having $a_2 \geqq |b_2|$. If also $a_3 \geqq a_2$, h is semi-reduced. But if $a_3 < a_2$, we repeat the process. Since the series of decreasing, positive integers $a_1, a_2, a_3, \ldots$ contains only a finite number of terms, we ultimately reach a semi-reduced form $[A, B, C]$. If $B=-A$, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ replaces it by $[A, A, C]$. Hence $-A < B \leqq A \leqq C$. As before we reach a reduced form satisfying (18).

42. No two reduced forms are equivalent.

THEOREM 52. *If two semi-reduced, positive forms are equivalent and distinct, they are one of the two pairs:*

(23) $$[a, a, c]\,, \quad [a, -a, c]\,;$$

(24) $$[a, b, a]\,, \quad [a, -b, a]\,.$$

Let $q=[a, b, c]$ and $Q=[A, B, C]$ be equivalent, semi-reduced, positive forms, whence

(25) $$c \geqq a \geqq |b|\,, \quad C \geqq A \geqq |B|\,.$$

We may take $a \geqq A$. There is an integral transformation (3) of determinant unity which replaces q by Q; then (5) and (6) hold. Since $(\alpha \mp \gamma)^2 \geqq 0$, $\alpha^2+\gamma^2 \geqq 2|\alpha\gamma|$. Hence

(26) $$A \geqq a\alpha^2 - a|\alpha\gamma| + a\gamma^2\,, \quad a \geqq A \geqq a|\alpha\gamma|\,,$$

(27) $$1 \geqq |\alpha\gamma|\,.$$

Unless $a=A$, we have $|\alpha\gamma|=0$ and

$$a > A = a\alpha^2 + c\gamma^2 \geqq a\alpha^2 + a\gamma^2 \geqq a\,,$$

since α and γ are not both zero in $\alpha\delta-\beta\gamma=1$. This contradiction gives $a=A$.

First, let one of $c>a$, $C>A$, hold. By interchanging q and Q if necessary, we may take $c>a$ without disturbing $a=A$. If $\gamma \neq 0$, then $c\gamma^2 > a\gamma^2$. Then the sign $\geqq$ is $>$ in the first relation (26) and hence in (27). Thus $\alpha\gamma=0$, $\alpha=0$, $a=A=c\gamma^2 \geqq c$. This contradiction gives $\gamma=0$. Then $\alpha\delta=1$, $\alpha=\delta=\pm 1$. By (6), $B-b=2a\alpha\beta$. By (25), $|b|$ and $|B|$ are $\leqq a$, whence $|B-b| \leqq 2a$, $|\beta| \leqq 1$. If $\beta=0$, $q=Q$. If $|\beta|=1$, then $|B-b|=2a$ and one of the numbers B, b is a and the other is $-a$. Since q and Q have equal discriminants, $C=c$. Hence the pair q, Q is the pair (23).

Second, let $c=a$, $C=A$. By $a=A$ and the equality of

the discriminants, $b^2=B^2$. Either $q=Q$ or the pair q, Q is the pair (24).

Conditions (18) are not satisfied by the second form (23), nor by one of (24). Hence we have

THEOREM 53. *Equivalent, positive, reduced forms are identical. Each class contains one and only one reduced form.*

43. Ambiguous and opposite forms. An integral form $q=[a, b, c]$ is called *ambiguous* if b is divisible by a. The *opposite* form to q is $q'=[a, -b, c]$. Evidently q' is semi-reduced when q is.

Theorem 52 shows that if q is semi-reduced, and equivalent to q', then q and q' are identical or coincide with one of the pairs (23), (24). Evidently $[a, 0, c]$ and $[a, \pm a, c]$ are all ambiguous forms if they are integral. If in $[a, b, a]$ we replace y by $y+x$, we obtain $[2a+b, 2a+b, a]$, which is ambiguous.

THEOREM 54. *Every integral, semi-reduced, positive form which is equivalent to its opposite is equivalent to an ambiguous form.*

THEOREM 55. *If an integral, positive form f is improperly equivalent to itself, f is equivalent to an ambiguous form.*

There exists an integral transformation T of determinant -1 which leaves f unaltered. There exists an integral transformation τ of determinant $+1$ which replaces f by a semi-reduced form q. Thus q is unaltered by $P=\tau^{-1}T\tau$. The transformation t which merely changes the sign of one variable has determinant -1 and replaces q by its opposite q'. Hence Pt is an integral transformation of determinant $+1$ which replaces q by q'. Our theorem therefore follows from Theorem 54.

44. Determination of all integral, reduced forms.

THEOREM 56. *There is only a finite number of integral, positive, reduced forms having a given negative discriminant* $-\Delta$.

By (20) there is a limited number of integers a. The same is true of b by (18). Each pair of integers a, b determines at most one integer c for which $4ac=\Delta+b^2$.

To obtain the reduced forms economically, let L be the largest integer $\leqq\sqrt{\Delta/3}$. By (20) and $|b|\leqq a$, $|b|\leqq L$. According as $\Delta\equiv 0$ or $3 \pmod 4$, the possible values of b are the even or odd integers, respectively, which occur in the set $0, \pm 1, \pm 2, \ldots, \pm L$. For each such b, $\frac{1}{4}(b^2+\Delta)$ is an integer; express it in all ways as a product ac, where $c\geqq a\geqq |b|$. When b is negative, we omit the cases in which $c=a$ or $a=-b$.

For example, let $\Delta=48$. Then $L=4$, $b=0, \pm 2, \pm 4$. For $b=0$, $ac=12$, $a=1, 2, 3$. The case $b=\pm 2$, $a=1$, $c=13$ is excluded by $a\geqq|b|$. For $b=\pm 4$, $ac=16$, $a=c=4$. Hence the reduced forms of discriminant -48 are $[1, 0, 12]$, $[2, 0, 6]$, $[3, 0, 4]$, $[4, 4, 4]$.

EXERCISES XIX

Verify that all reduced forms of discriminant $-\Delta$ are those listed in Exs. 1–8.

1. $\Delta=3$, $[1, 1, 1]$
2. $\Delta=4$, $[1, 0, 1]$
3. $\Delta=7$, $[1, 1, 2]$.
4. $\Delta=8$, $[1, 0, 2]$.
5. $\Delta=11$, $[1, 1, 3]$.
6. $\Delta=12$, $[1, 0, 3]$, $[2, 2, 2]$.
7. $\Delta=16$, $[1, 0, 4]$, $[2, 0, 2]$.
8. $\Delta=28$, $[1, 0, 7]$, $[2, 2, 4]$.
9. Prove by (18) and (20) that $ac\leqq\frac{1}{3}\Delta$ in a positive, reduced form.
10. Prove Theorem 56 by use of Ex. 9.

45. Automorphs. An integral transformation of determinant unity which leaves q unaltered is called an *automorph* of q.

THEOREM 57. *The only automorphs of* $a(x^2+y^2)$ *are*

$$T=\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}, \qquad S=\begin{pmatrix} 0 & \pm 1 \\ \mp 1 & 0 \end{pmatrix}.$$

The only automorphs of $a(x^2+xy+y^2)$ *are*

$$T\ ,\quad R=\begin{pmatrix} 0 & \mp 1 \\ \pm 1 & \pm 1 \end{pmatrix},\qquad R^{-1}=\begin{pmatrix} \pm 1 & \pm 1 \\ \mp 1 & 0 \end{pmatrix}.$$

If q *is a reduced, positive form distinct from these two, its only automorphs are* T.

We employ the proof of Theorem 52 with $Q=q$. If $c>a$, we have $\gamma=0$, $\alpha=\delta=\pm 1$, $a\alpha\beta=0$, whence $\beta=0$, and the only automorphs are T.

If $c=a$, then $b\geqq 0$ by (18). The argument leading to (27) may be applied also to C. Hence

$$|\alpha\gamma|=0 \text{ or } 1\ ,\qquad |\beta\delta|=0 \text{ or } 1\ .$$

If $\beta=0$, then $\alpha=\delta=\pm 1$, $0=B-b=2c\gamma\delta$, $\gamma=0$, and we get T. Hence except for T, we have $\beta\neq 0$, $\gamma\neq 0$.

If $\alpha=0$, then $\beta\gamma=-1$, $b=B=2c\gamma\delta-b$, $b=c\gamma\delta$. Then $\delta=0$ gives S. If $\delta\neq 0$, then $|\beta\delta|=1$, $b=c$, $\delta=\gamma$, and we get R.

If $\alpha\neq 0$ and $\delta=0$, then $\beta\gamma=-1$, $b=B=2a\alpha\beta-b$, $b=a\alpha\beta$, $|\alpha\gamma|=1$, $b=a$, $\alpha=\beta$, and we get R^{-1}.

There remains the case in which α, β, γ, δ are all numerically 1. This is excluded by $|\alpha\delta-1|=|\beta\gamma|=1$, $\alpha\delta=\pm 1$.

46. Proper representations. An integer m is said to be *representable properly* by an integral form $[a, b, c]$ of discriminant d if there exist relatively prime integers α and γ satisfying

$$a\alpha^2+b\alpha\gamma+c\gamma^2=m\ . \tag{28}$$

Then there exist integral solutions β, δ of

$$\alpha\delta-\beta\gamma=1\ . \tag{29}$$

If β', δ' satisfy (29), then $\alpha(\delta-\delta')=\gamma(\beta-\beta')$. Thus $\beta-\beta'$ is divisible by α, and

$$\beta=\beta'+t\alpha\ ,\quad \delta=\delta'+t\gamma \quad (t \text{ integral})\ .$$

Transformation (3) replaces $[a, b, c]$ by $[m, n, l]$, where m is given by (28), and n by (6). Hence $n = n' + 2tm$, where

$$n' = 2a\alpha\beta' + b(\alpha\delta' + \beta'\gamma) + 2c\gamma\delta'$$

is an integer. Let $m > 0$. There is a single integer t such that $0 \leqq n < 2m$. Then l is determined by

$$(30) \qquad n^2 - 4ml = d .$$

THEOREM 58. *Let* (α, γ) *be a proper representation of* $m > 0$ *by the integral form* $[a, b, c]$ *of discriminant* d. *Then integers* β, δ, n *can be determined in one and only one way to satisfy* (29), $0 \leqq n < 2m$, *and*

$$(31) \qquad n^2 \equiv d \pmod{4m} ,$$

such that the transformation $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ *replaces* $[a, b, c]$ *by the equivalent form* $[m, n, l]$ *in which* l *is determined by* (30).

A root n of (31) such that $0 \leqq n < 2m$ will be called a *minimum* root. A proper representation (α, γ) of m by $[a, b, c]$ therefore belongs to a unique minimum root of (31).

With n also $n + 2m$ is a root of (31). Hence the number of minimum roots is half the total number of roots.

To find all proper representations of m by $q = [a, b, c]$, we employ in turn all minimum roots n of (31). Determine l by (30) and write $Q = [m, n, l]$. If q and Q are not equivalent, Theorem 58 shows that there is no proper representation of m by q belonging to the chosen root n. Next, let n be such that $q \backsim Q$, and let T be one integral transformation of determinant 1 which replaces q by Q. If A is any automorph of q, evidently AT replaces q by Q. Conversely, if τ replaces q by Q, then τT^{-1} leaves q unaltered and is an automorph A of q, whence $\tau = AT$. If α and γ are the elements in the first column of the matrix of AT, evidently (28) holds and (α, γ) is a proper representation of m by q.

The form $[a, b, c]$ is called *primitive* if a, b, c have no common divisor >1. By Ex. XIX, 1, 2, every positive form of discriminant -3 or -4 is equivalent to x^2+xy+y^2 or x^2+y^2, respectively, and each is primitive. Thus Theorem 57 leads to

THEOREM 59. *Let $q=[a, b, c]$ be a positive, primitive, integral form of discriminant d. Let $w=2$ if $d<-4$, $w=4$ if $d=-4$, $w=6$ if $d=-3$, whence w is the number of automorphs of q. Let m be a positive integer. Employ in turn the minimum roots n of (31) and determine l by (30). If q is not equivalent to $Q=[m, n, l]$, there is no proper representation of m by q belonging to the root n. But if $q \backsim Q$, there are exactly w proper representations of m by q belonging to the root n.*

When $d=4D$, n in (31) is even. Write $n=2N$. Then

$$(32) \qquad N^2 \equiv D \pmod{m}.$$

Since $0 \leqq n < 2m$ is equivalent to $0 \leqq N < m$, we now employ all roots of (32).

THEOREM 60. *Let c be prime to M. Then*

$$(33) \qquad x^2 \equiv c \pmod{M}$$

has no root if M has an odd prime factor p such that $(c|p)=-1$; or if M is a multiple of 8 and $c \not\equiv 1 \pmod{8}$; or if M is a multiple of 4, but not of 8, and $c \equiv 3 \pmod{4}$. In all remaining cases, let r be the number of distinct odd primes dividing M. Then (33) has 2^r roots if M is not divisible by 4, 2^{r+1} roots if M is divisible by 4 but not by 8, and 2^{r+2} roots if M is divisible by 8.

This follows at once from Theorems 16 and 17.

47. Sum of two squares. We seek the number of proper representations of a positive, odd integer m by $q=x^2+y^2$. Here $d=-4$, $D=-1$. By (32), -1 must be a quadratic residue of each prime factor p of m, whence $p \equiv 1 \pmod{4}$. Let each of the r distinct prime factors of m be $\equiv 1 \pmod{4}$.

By Theorem 60, (32) has 2^r roots. If N is a chosen root, write $n=2N$, and determine l by (30). The positive form $[m, n, l]$ is equivalent to q, since q is the only reduced, positive form of discriminant -4. Hence Theorem 59 yields

THEOREM 61. *If m has r distinct prime factors each of the form $4k+1$, m has exactly $4 \cdot 2^r$ proper representations by x^2+y^2.*

If $m>1$, the following eight proper representations

$$(\pm x, y)\ ,\ (\pm x, -y)\ ,\ (y, \pm x)\ ,\ (-y\ , \pm x)$$

are distinct and lead to the same mode of expressing m as a sum of two squares.

THEOREM 62. *When m has r distinct prime factors each of the form $4k+1$, there are exactly 2^{r-1} ways of expressing m as a sum of two relatively prime squares, if the arrangement of the squares and the signs of their roots are disregarded. In particular, every prime $4h+1$ can be expressed as a sum of two squares in one and only one way.*

The last result concerning primes was known to A. Girard before 1625. Fermat stated that he could give a proof by descent. The first recorded proof is that by Euler in 1749.

EXERCISES XX

1. Show that $1+64$ and $16+49$ are the only ways to express 65 as a sum of two relatively prime squares. Hints: The only roots of $N^2 \equiv -1 \pmod{65}$ are ± 8 and ± 18. The forms $[65, 16, 1]$ and $[65, 36, 5]$ become x^2+y^2 by the respective transformations

$$\begin{pmatrix} 0 & 1 \\ -1 & -8 \end{pmatrix}, \quad \begin{pmatrix} -1 & -2 \\ 4 & 7 \end{pmatrix}.$$

The first columns in the inverse transformations give the proper representations $(-8, 1)$, $(7, -4)$.

2. If m is a positive integer all of whose r distinct prime factors are $\equiv 1$ or $3 \pmod 8$, there are exactly 2^{r+1} proper representa-

tions of m by x^2+2y^2. Every prime $\equiv 1$ or 3 (mod 8) is a sum of a square and the double of a square in one and only one way.*

3. A positive integer m, all of whose r distinct prime factors are $\equiv 1$ (mod 3), has exactly 2^{r+1} proper representations by x^2+3y^2 Every prime $3h+1$ is a sum of a square and the triple of a square in one and only one way*.

4. For m as in Ex. 3, m has exactly $6\cdot 2^r$ proper representations by $q=x^2+xy+y^2$. In the six representations

$$(\pm x, \pm y), \quad (\pm x \pm y, \mp x), \quad (\mp y, \pm x \pm y).$$

just one of $x, y, x+y$ is even. Let $(\pm s, \pm t)$ be the two of the six in which t is even. Write $t=2\eta$, $s=\xi-\eta$. Then $s^2+st+t^2=\xi^2+3\eta^2$. The $2\cdot 2^r$ pairs $(\pm\xi, \pm\eta)$ coincide with the representations of m by [1, 0, 3] in Ex. 3.

5. A positive, odd m, all of whose r distinct prime factors are $\equiv 1$, 2, or 4 (mod 7), has exactly 2^{r+1} proper representations by x^2+7y^2.

48. Kronecker's symbol. Let $d\equiv 0$ or 1 (mod 4). If p is a prime dividing d, let $(d|p)=0$. Let $(d|2)=1$ if $d\equiv 1$ (mod 8), $(d|2)=-1$ if $d\equiv 5$ (mod 8). If p is an odd prime not dividing d, let $(d|p)$ be Legendre's symbol (§ 21) Let $(d|1)=1$. Finally, if the p_i are primes, let

$$(34)\qquad (d|m)=\prod_{i=1} (d|p_i), \quad m=\prod_{i=1} p_i.$$

Hence $(d|k)$ is defined for every positive integer k.

EXERCISES XXI

1. $(d|k)=0$ if and only if d and k have a common factor >1, otherwise $(d|k)=\pm 1$

2. If $k>0$, $l>0$, $(d|kl)=(d|k)(d|l)$.

3. Kronecker's and Jacobi's symbols are equal for all values of d and k for which both are defined.

* Stated by Fermat in 1654, *Œuvres*, II (1894), pp. 313, 403–4. The first published proofs were by Euler, *Novi comm. acad. petrop.*, VIII (1763), 105–28; *Opera omnia* (ser 1), II. 558–75

49. Number of roots of a quadratic congruence.

THEOREM 63. *Let* $d \equiv 0$ *or* 1 (*mod* 4). *If m is positive and prime to d, the number of solutions of*

(35) $$x^2 \equiv d \pmod{4m}$$

is $2\Sigma(d|f)$, *summed for the positive divisors f, lacking square factors, of m.*

I. Let $d \equiv 1 \pmod 4$. Let p^h be the highest power of a prime p dividing $4m$. By Theorem 17, the number of roots of

(36) $$x^2 \equiv d \pmod{p^h}$$

is

$$1+(d|p) \text{ if } p>2\ ;$$
$$2 \text{ if } p=2,\ h=2\ (m \text{ odd})\ ;$$
$$2[1+(d|p)] \text{ if } p=2,\ h>2\ (m \text{ even})\ .$$

Then by Theorem 16, the number of solutions of (35) is

(37) $$2\Pi[1+(d|p)]=2\Sigma(d|f)\ ,$$

where the product extends over all distinct prime factors p of m, and the equality holds by Ex. XXI, 2.

II. Let $d \equiv 0 \pmod 4$. Here m is odd. Evidently $x^2 \equiv d \pmod 4$ has two roots 0 and 2. If p^h is the highest power of a prime p dividing m, (36) has $1+(d|p)$ roots. Hence the number of roots of (35) is (37).

50. Number of representations by positive forms.

THEOREM 64. *Let m be positive and prime to d. The number* $\psi(m)$ *of all representations of m by the various forms of a representative system of positive, primitive, integral forms of discriminant d (a single form being chosen from each class) is* $w\Sigma(d|\mu)$, *where* μ *ranges over all positive divisors of m, and w was defined in Theorem* 59.

By Theorem 63, the number of minimum roots n of (35) is $\Sigma(d|f)$. To each n corresponds a unique l by (30)

such that $[m, n, l]$ has the discriminant d, is positive, and is primitive since a common divisor of m and n would divide d. Hence $[m, n, l]$ is equivalent to a single form of the representative system. Since w is the number of automorphs of $[m, n, l]$, there are exactly w proper representations of m by this form belonging to the chosen root n (Theorem 59). Hence the number of proper representations of m by the various forms of the representative system is $w\Sigma(d|f)$.

If m is represented by $[a, b, c]$ by integers x and y whose g.c.d. g exceeds 1, the representation is called *improper*. Then m/g^2 is represented properly by $[a, b, c]$ by the relatively prime integers x/g and y/g. The converse is true. Hence the number of all representations of m by the representative system is

$$\psi(m) = w\sum_{g^2}\sum_{f}(d|f)\ ,$$

where g^2 ranges over all square factors (including 1) of m, while f ranges over all positive divisors, free of square factors >1, of m/g^2.

Write μ for fg^2. Then μ is a positive divisor of m, and

$$(d|\mu) = (d|f)(d|g^2) = (d|f)$$

by (34) and Ex. XXI, 2. Hence every term of the double sum is a unique term of $\Sigma(d|\mu)$, where μ ranges over all positive divisors of m. Conversely, any such μ can be expressed uniquely in the form fg^2, where f has no square factor >1. Then g^2 divides m, and f divides m/g^2. Thus every term of $\Sigma(d|\mu)$ is a unique term of the double sum.

In a different form, Theorem 64 was first obtained by Dirichlet in 1840 and used in his elaborate, analytic investigation of a formula for the number of classes of forms of a given discriminant.

51. Sum of two squares. We apply Theorem 64 with $d=-4$ and m any positive, odd integer. By (34) we may delete the factor 4 from $(-4|\mu)$. We may take x^2+y^2 as the single form in the representative system. For the case $k=0$, we therefore have

THEOREM 65. *The number of all representations of $2^k m$ (where m is positive and odd) by x^2+y^2 is $4E$, where $E=\Sigma(-1)^{\frac{1}{2}(\mu-1)}$, summed for all positive divisors μ of m. Hence E is the excess of the number of divisors $\equiv 1 \pmod 4$ of m over the number of divisors $\equiv 3 \pmod 4$ of m.*

Next, if $2n=x^2+y^2$, we have $x+y=2X$, $x-y=2Y$, where X and Y are integers; whence $n=X^2+Y^2$. The correspondence between the pairs x, y and X, Y is one to one. This completes the proof of Theorem 65, which was first obtained by Jacobi in his *Fundamenta nova theoriae functionum ellipticarum* (1829).

EXERCISES XXII

1. If m is positive and odd, the number of all representations of $2^k m$ by x^2+2y^2 is double the excess of the number of divisors $\equiv 1$ or $3 \pmod 8$ of m over the number of divisors $\equiv 5$ or $7 \pmod 8$ of m.

2. The number of representations of any positive n by $q=x^2+xy+y^2$ is $6E(n)$ where $E(n)$ is the excess of the number of divisors $3h+1$ of n over the number of divisors $3h+2$. If $n=2^k m$, m odd, then $E(n)=0$ when k is odd, $E(n)=E(m)$ when k is even. Hints: If $q=3r$, then $(x-y)^2\equiv 0 \pmod 3$, $x=X+2Y$, $y=X-Y$, and $q=3Q$, $Q=X^2+XY+Y^2=r$. If q is even, then $x=2X$, $y=2Y$, $q=4Q$.

3. If m is positive and odd, the number of representations of $2^k m$ by $f=x^2+3y^2$ is zero if k is odd, $2E(m)$ if $k=0$, and $6E(m)$ if k is even and >0, for E as in Ex. 2. Hints: If $f=8n$, then $x=2X$, $y=2Y$, $X^2+3Y^2=2n$. If $f=2l$, then $y+x=2X$, $y-x=2Y$, $f=4q$, $q=X^2+XY+Y^2$, $2q=l$. Hence $f\neq 2m$, and the number of representations of $4m$ by f is the number $6E(m)$ of representations of m by q (Ex 2.).

4. If m is positive and odd, $x^2+3y^2=4m$ has $E(m)$ solutions in positive odd integers. Apply Ex. 3 with $k=2$ and $k=0$

5. If m is positive and odd, the number of representations of $2^k m$ by x^2+4y^2 is $2E$ if $k=0$, 0 if $k=1$, $4E$ if $k\geqq 2$, for E in Theorem 65.

6. The number of representations of $n>0$ by $q=x^2+xy+2y^2$ is double the excess $e(n)$ of the number of divisors $\equiv 1$, 2, or 4 (mod 7) of n over the number of divisors $\equiv 3$, 5, or 6 (mod 7) of n. Hint. If $q\equiv 0$, then $x\equiv 3y$ (mod 7). Thus $x=-X+3Y$, $y=2X+Y$, and $q=7Q$, $Q=X^2+XY+2Y^2$.

7. In Ex. 6, $e(2^a m)=(a+1)e(m)$ if m is odd. If t is prime to 3, $e(3^b t)$ is 0 if b is odd, but $=e(t)$ if b is even. Hint. If $q\equiv 0$, then $q\equiv(y-x)^2+y^2$, $y\equiv x\equiv 0$ (mod 3), $q=9Q$, and $e(9N)=e(N)$ for every N.

8. Hence if $n=2^a 3^b t$, where t is prime to 6, $e(n)=0$ when b is odd, $e(n)=(a+1)e(t)$ when b is even.

9. The number of representations by x^2+7y^2 of a positive, odd m is $2e(m)$, that of $2m$ is zero, that of $4k$ is $2e(k)$, for e in Ex. 6. Hint: If $x^2+7y^2=2l$, then $x=y+2z$, $l=2(2y^2+yz+z^2)$.

10. By Exs. 8, 9, the number of representations by x^2+7y^2 of $2^a 3^b t$ (t prime to 6) is 0 if b is odd, $2|a-1|e(t)$ if b is even.

11. If m is odd and positive, $x^2+7y^2=8m$ has exactly $e(m)$ solutions in positive integers. Hint: Take $k=2m$ in Ex. 9 and show that $e(2m)=2e(m)$.

12. The number of representations by $q=x^2+xy+3y^2$ of $m>0$ is double the excess of the number of divisors $\equiv 1$, 3, 4, 5, or 9 (mod 11) over the number of divisors $\equiv 2, 6, 7, 8, 10$ (mod 11). Hint. If $q\equiv 0$, then $2x+y\equiv 0$ (mod 11). Replacing x by $x+6y$ and y by $-2x-y$ in q, we get $11q$.

13. Discuss the remaining* discriminants -19, -27, -43, -67, and -163 for which there is a single reduced, positive, primitive form.

52. Why genera are introduced here. Hitherto we have found the number of representations only when there

* In *Bull. Amer. Math. Soc.*, XVII (1911), 534–37, the author proved there are no more to $-1,500,000$.

is a single reduced, primitive form. In case there are two or more reduced, positive, primitive forms f_i of discriminant d, we require arithmetical invariants which serve to distinguish the numbers represented by f_1 from those represented by f_2, f_3, ... Such invariants, called *characters*, will be next defined. They will differentiate the numbers represented by the separate f_i in case no two of the f_i belong to the same genus.

THEOREM 66. *Every integral, primitive form q represents properly an integer prime to any assigned integer n.*

Let $q(x, y)=ax^2+bxy+cy^2$, where the g.c.d. of a, b, c is 1. Let p be any prime factor of n. If a is not divisible by p, take x prime to p, and y divisible by p; we get a value of q prime to p. If c is not divisible by p take x divisible by p, and y prime to p. If both a and c are divisible by p, then b is prime to p, and we take x and y both prime to p. Hence if $p_1, \ldots, p_k$ are the distinct prime factors of n, there exist integers x_i, y_i such that $q(x_i, y_i)$ is prime to p_i. By Theorem 15, there exist integers x and y such that

$$x\equiv x_1,\ y\equiv y_1 \pmod{p_1},\ \ldots,\ x\equiv x_k,\ y\equiv y_k \pmod{p_k}\ .$$

Since $q(x, y)$ is prime to each p_i, it is prime to n. The same is true after deleting from x and y any common factor.

53. Characters. Consider an integral, primitive form

(38) $\quad q=ax^2+2bxy+cy^2$ of *determinant* $D=b^2-ac$,

whose middle coefficient $2b$ is even. By Theorem 66, q represents integers n prime to $2D$.

THEOREM 67. *If p_1, p_2, . . . are the distinct odd prime factors of D, then $(n \mid p_i)$ has the same value for all integers n prime to $2D$ which are represented by q. The same is true of*

$$\delta=(-1)^{\frac{1}{2}(n-1)} \text{ if } D\equiv 0 \text{ or } 3 \pmod 4\ ,$$

$$\epsilon=(-1)^{\frac{1}{8}(n^2-1)} \text{ if } D\equiv 0 \text{ or } 2 \pmod 8\ ,$$

$$\delta\epsilon \text{ if } D\equiv 0 \text{ or } 6 \pmod 8\ .$$

These symbols $(n|p_i)$ and such of δ, ϵ, $\delta\epsilon$ as occur for the given D are called *characters* of the form q. Note that $\epsilon=(2|n)$, and when n is positive, $\delta=(-1|n)$.

To prove Theorem 67, let

$$n=au^2+2buv+cv^2\ ,\quad m=ar^2+2brs+cs^2\ .$$

Then

$$(39)\quad nm=x^2-Dy^2\ ,\ x=aur+bus+brv+cvs,\ y=us-rv\ .$$

Let n and m be prime to $2D$ and hence to any odd prime factor p of D. Then $nm\equiv x^2 \pmod{p}$, whence*

$$(nm|p)=1\ ,\quad (n|p)=(m|p)\ ,$$

which proves the theorem for the symbols $(n|p_i)$.

Let $D\equiv 3 \pmod{4}$. Then $nm\equiv x^2+y^2 \pmod{4}$. But n and m are odd. Hence one of x, y is even and the other is odd. Thus

$$nm\equiv 1\ ,\quad n\equiv m \pmod{4}\ ,\quad \delta'=(-1)^{\frac{1}{2}(m-1)} \text{ equals } \delta\ .$$

Let $D\equiv 2 \pmod{8}$. Then x is odd in (39). According as y is even or odd, $nm\equiv +1$ or -1, $n\equiv \pm m \pmod{8}$. Hence

$$n^2\equiv m^2 \pmod{16}\ ,\quad \epsilon'=(-1)^{\frac{1}{8}(m^2-1)} \text{ equals } \epsilon\ .$$

Let $D\equiv 6 \pmod{8}$. Then $nm\equiv 1$ or 3, $n\equiv m$ or $3m \pmod{8}$, whence $n^2\equiv m^2$ or $9m^2 \pmod{16}$. For the first alternative, $\delta'=\delta$, $\epsilon'=\epsilon$, as before. For the second alternative,

$$\delta=(-1)^m\delta'\ ,\quad \epsilon=(-1)^{m_1}\epsilon'\ ,\quad \delta\epsilon=\delta'\epsilon'\ ,$$

whence $\delta\epsilon$ is a character.

If $D\equiv 0 \pmod{4}$, $nm\equiv x^2\equiv 1$, $n\equiv m \pmod{4}$, $\delta=\delta'$.

If $D\equiv 0 \pmod{8}$, $nm\equiv x^2\equiv 1$, $n\equiv m \pmod{8}$, $\epsilon=\epsilon'$.

* Also if n, m are any integers prime to p which are represented by q.

All primitive forms (38) of the same determinant D (or same discriminant $4D$) each of whose characters has an assigned value are said to form a *genus*. Since two equivalent forms represent the same numbers and hence have the same characters, they belong to the same genus. In other words, each genus is composed of one or more classes of forms.

For example, there are just four positive, reduced, primitive forms q of discriminant -96 $(D=-24)$:

q	$(n\|3)$			Computed for $n\equiv$
[1, 0, 24]	+1	+1	+1	1
[3, 0, 8]	−1	−1	−1	11
[4, 4, 7]	+1	−1	+1	7
[5, 2, 5]	−1	+1	−1	5

Hence the four forms lie in four different genera. By Theorem 64, if n is positive and prime to 6, the number of representations of n by the four forms is $2\Sigma(-6\,|\,\mu)$, where μ ranges over the positive divisors of n. According as $n\equiv 1$, 11, 7, or 5 (mod 12), the representations are all by the first, second, third, or fourth form, respectively. For, $(n\,|\,3)$ and δ then have the values displayed.

EXERCISES XXIII

[The number of representations of n by f is denoted by $f(n)$ Use Table I.]

1. If m is positive and prime to 10, the number of representations of 2^r5^sm by x^2+5y^2 is $[1+(m\,|\,5)]E$, and that by $2x^2+2xy+3y^2$ is $[1-(m\,|\,5)]E$, if r is even, but *vice versa* if r is odd, where $E=\Sigma(-5\,|\,\mu)$, μ ranging over the divisors of m. Hence E is the excess of the number of divisors $\equiv 1$, 3, 7, or 9 (mod 20) of m over the number of divisors $\equiv 11$, 13, 17, or 19 (mod 20) of m.

2. Let $f=x^2+6y^2$, $q=2x^2+3y^2$. If m is positive and prime to 6, $f(m)=[1+(m\,|\,3)]E$, $q(m)=[1-(m\,|\,3)]E$, where $E=\Sigma(-6\,|\,\mu)$, summed for the divisors μ of m Thus E is the excess of the number of divisors $\equiv 1$, 5, 7, or 11 (mod 24) of m over the number of

divisors $\equiv 13, 17, 19$, or 23 (mod 24). For $k=2$ or 3, $f(kn)=q(n)$, $q(kn)=f(n)$. Hence we know $f(N)$ and $q(N)$ for every N.

TABLE I

REDUCED, POSITIVE, PRIMITIVE FORMS OF DISCRIMINANT $-\Delta$ WITH A SINGLE CLASS IN EACH GENUS

3	1, 1, 1	67	1, 1, 17	147	1, 1, 37	240	1, 0, 60
4	1, 0, 1	72	1, 0, 18		3, 3, 13		3, 0, 20
7	1, 1, 2		2, 0, 9	148	1, 0, 37		4, 0, 15
8	1, 0, 2	75	1, 1, 19		2, 2, 19		5, 0, 12
11	1, 1, 3		3, 3, 7	160	1, 0, 40	267	1, 1, 67
12	1, 0, 3	84	1, 0, 21		4, 4, 11		3, 3, 23
15	1, 1, 4		2, 2, 11		5, 0, 8	280	1, 0, 70
	2, 1, 2		3, 0, 7		7, 6, 7		2, 0, 35
16	1, 0, 4		5, 4, 5	163	1, 1, 41		5, 0, 14
19	1, 1, 5	88	1, 0, 22	168	1, 0, 42		7, 0, 10
20	1, 0, 5		2, 0, 11		2, 0, 21	288	1, 0, 72
	2, 2, 3	91	1, 1, 23		3, 0, 14		4, 4, 19
24	1, 0, 6		5, 3, 5		6, 0, 7		8, 0, 9
	2, 0, 3	96	1, 0, 24	180	1, 0, 45		8, 8, 11
27	1, 1, 7		3, 0, 8		2, 2, 23	312	1, 0, 78
28	1, 0, 7		4, 4, 7		5, 0, 9		2, 0, 39
32	1, 0, 8		5, 2, 5		7, 4, 7		3, 0, 26
	3, 2, 3	99	1, 1, 25	187	1, 1, 47		6, 0, 13
35	1, 1, 9		5, 1, 5		7, 3, 7	315	1, 1, 79
	3, 1, 3	100	1, 0, 25	192	1, 0, 48		5, 5, 17
36	1, 0, 9		2, 2, 13		3, 0, 16		7, 7, 13
	2, 2, 5	112	1, 0, 28		4, 4, 13		9, 9, 11
40	1, 0, 10		4, 0, 7		7, 2, 7	340	1, 0, 85
	2, 0, 5	115	1, 1, 29	195	1, 1, 49		2, 2, 43
43	1, 1, 11		5, 5, 7		3, 3, 17		5, 0, 17
48	1, 0, 12	120	1, 0, 30		5, 5, 11		10, 10, 11
	3, 0, 4		2, 0, 15		7, 1, 7	352	1, 0, 88
51	1, 1, 13		3, 0, 10	228	1, 0, 57		4, 4, 23
	3, 3, 5		5, 0, 6		2, 2, 29		8, 0, 11
52	1, 0, 13	123	1, 1, 31		3, 0, 19		8, 8, 13
	2, 2, 7		3, 3, 11		6, 6, 11	372	1, 0, 93
60	1, 0, 15	132	1, 0, 33	232	1, 0, 58		2, 2, 47
	3, 0, 5		2, 2, 17		2, 0, 29		3, 0, 31
64	1, 0, 16		3, 0, 11	235	1, 1, 59		6, 6, 17
	4, 4, 5		6, 6, 7		5, 5, 13		

3. Let $f=x^2+8y^2$, $q=3x^2+2xy+3y^2$. If m is positive and odd, $f(m)=[1+(-1|m)]E$, $q(m)=[1-(-1|m)]E$, where $E=\Sigma(-2|\mu)$, summed for the divisors μ of m. Let $h=x^2+2y^2$. Evidently $f(2m)=0$, $f(4n)=h(n)$. If q is even, we may replace x by $x+y$,

and y by $y-x$ and get $q=4(x^2+2y^2)$, whence $q(2m)=0$, $q(4n)=h(n)$. For E and $h(n)$, see Ex. XXII, 1.

4. Let $f=x^2+9y^2$, $q=2x^2+2xy+5y^2$, $l=x^2+y^2$. For every r, evidently $f(3r-1)=0$, $f[3(3r\pm 1)]=0$, $f(9r)=l(r)$. It remains to find $f(N)$ for $N\equiv 1 \pmod 3$. Let $N=2^k n$ (n odd). Evidently $f(4r)=f(r)$. If k is even, $1\equiv N\equiv n \pmod 3$, $n=6s+1$, $f(N)=f(n)=2E$, where $E=\Sigma(-1|\mu)$ is the excess of the number of divisors $\equiv 1 \pmod 4$ of n over the number of divisors $\equiv 3 \pmod 4$. In fact, $q\neq n$, whence $f=n$. But $4E=l(n)$, whence $f(N)=\frac{1}{2}l(N)$. But if k is odd, $1\equiv N\equiv 2n \pmod 3$, $n=6s-1$,

$$f(N)=f(2n)=q(n)=2E=\tfrac{1}{2}l(n)=\tfrac{1}{2}l(N),$$

since $2q=(2x+y)^2+9y^2$. Hence $q(r)=f(2r)$.

5. Let $f=x^2+10y^2$, $q=2x^2+5y^2$, m odd. If $m\equiv\pm 1 \pmod 5$, $q(m)=0$, $f(m)=2E$, $E=\Sigma(-10|\mu)$, summed for the divisors μ of m. If $m\equiv\pm 2 \pmod 5$, $f(m)=0$, $q(m)=2E$. Evidently $f(2n)=q(n)$, $q(2n)=f(n)$. Hence our results hold also when m is even if, in E, μ ranges over the odd divisors of m. Finally, $f(5r)=q(r)$, $q(5r)=f(r)$ for every r.

6. Let $f=x^2+12y^2$, $q=3x^2+4y^2$, $h=x^2+3y^2$, m prime to 6. Use character δ, and E and $h(r)$ in Ex. XXII, 2, 3. If $m\equiv 1 \pmod 4$, $f(m)=2E$, $q(m)=0$. If $m\equiv 3 \pmod 4$, $f(m)=0$, $q(m)=2E$. For any r, $f(4r)=q(4r)=h(r)$, $f(2m)=q(2m)=0$, $f(3r)=q(r)$, $q(3r)=f(r)$.

7. Let $f=x^2+13y^2$, $q=2x^2+2xy+7y^2$, m odd. If $(m|13)=1$, viz., if $m\equiv 1$, 3, 4, 9, 10, or 12 (mod 13), $q(m)=0$, $f(m)=2E$, $E=\Sigma(-13|\mu)$, summed for the divisors μ of m. If $(m|13)=-1$, $f(m)=0$, $q(m)=2E$. The same holds also for m even if μ ranges over only odd divisors of m, since $f(2r)=q(r)$, $q(2r)=f(r)$. Evidently $f(13r)=f(r)$, $q(r)=f(2r)$, whence $q(13r)=q(r)$.

8. Discuss discriminants -60, -64, -72, -88.

54. Odd discriminant *d*. Let $f=ax^2+bxy+cy^2$ be an integral, primitive form of odd discriminant d, whence b is odd. By Theorem 66, f represents an integer prime to $2d$. To secure notations conforming with (38), consider $q=2f$.

The determinant of q is d. Let r and s be prime to $2d$ and be represented by f. Then $n=2r$ and $m=2s$ are represented by q. By (39), $4rs=x^2-dy^2$. Hence if p_i is any prime factor of d, $(rs|p_i)=1$ and $(r|p_i)=(s|p_i)$. Thus $(r|p_i)$ are the (only) *characters* of f.

All primitive forms f with the same odd discriminant d, each of whose characters $(r|p_i)$ has an assigned value, form a *genus*.

For example, the positive, reduced forms of discriminant -15 are $f=x^2+xy+4y^2$ and $h=2x^2+xy+2y^2$. Let m be positive and prime to 2, 3, and 5. Since f represents 1, $f=m$ requires

$$(m|3)=(m|5)=1\ , \quad m\equiv 1 \text{ or } 4 \pmod{15}\ .$$

Next, $h=17$ when $x=-3$, $y=1$, and $(17|3)=(17|5)=-1$. Hence $h=m$ requires

$$(m|3)=(m|5)=-1\ , \quad m\equiv 2 \text{ or } 8 \pmod{15}\ .$$

Hence if $m\equiv 7$, 11, 13, or 14 (mod 15), m is represented by neither f nor h. Let $E=\Sigma(-15|\mu)$, where μ ranges over the divisors of m. By Theorem 64, $f(m)=2E$ and $h(m)=0$ if $m\equiv 1$ or 4 (mod 15), while $f(m)=0$, $h(m)=2E$ if $m\equiv 2$ or 8 (mod 15).

EXERCISES XXIV

1. Verify the preceding example as follows. If f is odd, then x is odd, $y=2\eta$, $f=\xi^2+15\eta^2$, $\xi=x+\eta$. For ξ prime to 15, $\xi^2\equiv 1$ or 4 (mod 15). If h is odd and prime to 15, then $x=\xi+\eta$, $y=\xi-\eta$, $h=5\xi^2+3\eta^2\equiv 2$ or 8 (mod 15).

2. If $f\equiv 0$, then $x\equiv y \pmod 3$, $x=y-3z$. In $\frac{1}{3}f=2y^2-3yz+3z^2$, we replace y by $y+z$ and get h, whence $f(3r)=h(r)$. Similarly, $h(3r)=f(r)$, $f(5r)=h(r)$, $h(5r)=f(r)$. Hence $f(3^r5^sm)=f(m)$ or $h(m)$, according as $r+s$ is even or odd.

3. $f(2r)=2h(r)-F$, where $F=0$ if r is odd, $F=f(\frac{1}{2}r)$ if r is even. For, if x and y are odd, $x=y-2z$, $\frac{1}{2}f=3y^2-3yz+2z^2$. Replacing z by $z+y$, we get a form of type h with y odd. But the number of solutions of $h=r$ with $y=2Y$ is 0 if r is odd and is $f(\frac{1}{2}r)$ if r is even.

4. $h(2r)=2f(r)-H$, where $H=0$ if r is odd, $H=h(\frac{1}{2}r)$ if r is even. Treat* h for x even, and for x odd, $y=2Y$, whence $\frac{1}{2}h$ is of type f with x odd. But f with x even is $2h$.

5. From Exs. 3, 4 prove by induction

$$f(2^{2n}r)=(2n+1)f(r)\ , \quad f(2^{2n-1}r)=2nh(r)$$

and formulas derived from these by interchanging f and h.

6. Discuss discriminants -35, -51, -75.

55. Positive forms with a single class in each genus. Let each genus of discriminant $-\Delta$ $(\Delta>0)$ contain a single reduced, positive, primitive, integral form. All cases with $\Delta<400$ are tabulated on page 85. We shall show how to construct this table and an extension of it. It is only for forms of such discriminants that we can find a simple expression for the number of all representations as in Exercises XXII-XXIV.

Let Δ be odd. If $\Delta=8k-1>15$, both of $[2, \pm 1, k]$ are reduced, represent the same numbers, and hence are in the same genus. Hence let $\Delta\equiv 3 \pmod 8$. Write

$$T_j=\tfrac{1}{4}[\Delta+(2j+1)^2]\ .$$

Thus T_j is odd. *T_0 must be a prime or the square of a prime.* Otherwise, $T_0=ac$, $c>a>1$, and $[a, \pm 1, c]$ are both positive, reduced, primitive forms of discriminant $-\Delta$.

Suppose that T_1 is neither a prime nor the square of a prime. First, let $T_1=3^n q$, where $q>1$ and q is not divisible by 3, whence $q\geqq 5$. If $n>1$, let L be the larger and S the smaller of 3^n and q; then $[S, \pm 3, L]$ are both positive, reduced, primitive forms of discriminant $-\Delta$. But if $n=1$ and q is composite, then $q=rs$, $s\geqq r\geqq 5$, and $[r, \pm 3, 3s]$ are both reduced and primitive. Second, if $T_1=3^5$, we use $[13, \pm 5, 19]$. Third, if $T_1=3^n$, $n>5$, we use $[27, \pm 15,$

* We avoid the case y odd, $x=2X$, whence $\frac{1}{2}h=f$, since f with y even is of type $\xi^2+15\eta^2$

$2+3^{n-2}]$. Finally, if $T_1 = ac$, $c > a > 3$, use $[a, \pm 3, c]$. Hence *T_1 must be a prime, the square of a prime, the triple of a prime, 3^3, or 3^4.*

These two tests in italics serve to exclude nearly every odd $\Delta < 400$ not listed in the table

At the author's suggestion, S. B. Townes made a more extended examination. Apart from primes p and their squares, he showed that $T_2 = 5p$, 5^2, or 5^3; $T_3 = 7p$ or 7^2; $T_4 = 3p$ or 99; if $j > 4$, $T_j = Pp$, where P is a product of distinct prime factors of $2j+1$. For T_i every mentioned p exceeds $2i+1$. By means of these results he verified that, when $400 < \Delta < 23000$, there is a single class of positive, primitive forms of odd discriminant $-\Delta$ if and only if $\Delta = 403$, 427, 435, 483, 555, 595, 627, 715, 795, 1,155, 1,435, 1,995, 3,003, 3,315

Next, let $\Delta = 4D$. For the 36 values of D with $D < 100$ see the table. For $100 < D < 100{,}000$, the 29 values of D are 102, 105, 112, 120, 130, 133, 165, 168, 177, 190, 210, 232, 240, 253, 273, 280, 312, 330, 345, 357, 385, 408, 462, 520, 760, 840, 1,320, 1,365, 1,848

In 1778 Euler found that these 65 *idoneal* numbers D are the only ones $< 10{,}000$ having the property that, if $ab = D$, every number represented by $f = ax^2 + by^2$ (with ax prime to by) is a prime, the square of a prime, the double of a prime, or a power of 2 If a number is represented by f in a single way, it is a prime.

56. Criterion for equivalence of forms.

THEOREM 68 *Two forms $[a, b, c]$ and $[A, B, C]$ with $A \neq 0$ are equivalent if and only if their discriminants are equal and there exist two integers α and γ satisfying*

$$(40) \qquad A = a\alpha^2 + b\alpha\gamma + c\gamma^2 ,$$

$$(41) \qquad 2a\alpha + (b+B)\gamma \equiv 0 , \quad (b-B)\alpha + 2c\gamma \equiv 0 \pmod{2A}$$

The advantage of this criterion is that it demands two integers satisfying one equation and two simple congruences, while the definition of equivalence demands four integers which satisfy the same equation and two additional equations.

I. Let the forms be equivalent. Then there exist integers $\alpha, \beta, \gamma, \delta$ satisfying $\alpha\delta-\beta\gamma=1$ and (5) and (6). To (6) add $b=b(\alpha\delta-\beta\gamma)$ and insert the resulting value of $b+B$ into the left member of (41_1); we get

$$2a\alpha(1+\beta\gamma)+2b\alpha\delta\gamma+2c\gamma^2\delta\ .$$

Replacing $1+\beta\gamma$ by $\alpha\delta$, we get $2\delta A$ by (40). Similarly, the left member of (41_2) is found to reduce to $-2\beta A$.

II. Let (40) and (41) hold. Denote the integral quotients of the sums in (41) by $2A$ by δ and $-\beta$, whence

$$2a\alpha+(b+B)\gamma=2\delta A\ ,\quad (b-B)\alpha+2c\gamma=-2\beta A\ .$$

Multiply these by α and γ, respectively, and add; we get

$$2A=2A(\alpha\delta-\beta\gamma)\ ,\quad \alpha\delta-\beta\gamma=1\ .$$

Next, multiply them by β and δ, and add; we get (6). Hence $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ has determinant unity and replaces $[a, b, c]$ by $[A, B, t]$. Since the latter has the same discriminant as $[A, B, C]$, we have $t=C$.

EXERCISES XXV

1. $[4, 6, 1]\backsim[4, -2, -1]$.

2. $f=[a, b, c]\backsim[\pm 1, B, C]$ if and only if they have the same discriminant and f represents ± 1.

CHAPTER VI

CERTAIN DIOPHANTINE EQUATIONS

57. We saw in § 30 that the integral solutions of an equation are usually not all given by a single integral formula, but require several such formulas. This fact is brought out emphatically by the following important investigation.

THEOREM 69. *All integral solutions of*

$$(1) \qquad x^2-my^2=zw$$

are given by

$$x=\pm\rho(e\xi u+f\eta u-f\xi v-g\eta v)\ , \quad y=\rho(\xi v+\eta u)\ ,$$
$$z=\rho(e\xi^2+2f\xi\eta+g\eta^2)\ , \quad w=\rho(eu^2-2fuv+gv^2)\ ,$$

where ρ, ξ, η, u, v are arbitrary integers, while e, f, g take only the finite sets of integral values such that the forms

$$(2) \qquad F(\xi,\eta)=e\xi^2+2f\xi\eta+g\eta^2$$

are representative forms, just one being chosen from each class of forms of determinant

$$(3) \qquad f^2-eg=m\ .$$

This solution is unaltered when we merely change the signs of u, v, ρ, e, f, g. Hence if $m<0$, we may restrict F to positive, reduced forms.

Ex. 1. For $m=-1$, then $F=\xi^2+\eta^2$ and the theorem states that all integral solutions of $x^2+y^2=zw$ are given by

$$(4) \quad x=\pm\rho(\xi u-\eta v)\ ,\ y=\rho(\xi v+\eta u)\ ,\ z=\rho(\xi^2+\eta^2)\ ,\ w=\rho(u^2+v^2)$$

Ex. 2. For $m=-5$, F is $\xi^2+5\eta^2$ or $2\xi^2+2\xi\eta+3\eta^2$ and the theorem states that all integral solutions of $x^2+5y^2=zw$ are given by the following two sets of formulas

$$(5)\quad x=\pm\rho(\xi u-5\eta v)\ ,\quad y=\rho(\xi v+\eta u)\ ,\quad z=\rho(\xi^2+5\eta^2)\ ,\quad w=\rho(u^2+5v^2)\ ;$$

$$(6)\quad \begin{cases} x=\pm\rho(2\xi u+\eta u-\xi v-3\eta v)\ ,\quad y=\rho(\xi v+\eta u)\ ,\\ z=\rho(2\xi^2+2\xi\eta+3\eta^2)\ ,\quad w=\rho(2u^2-2uv+3v^2)\end{cases}$$

Proof of Theorem 69. Since ρ takes care of any common factor of x, y, z, w, we may assume henceforth that the latter have no common factor >1. Let Δ be the g.c.d. of x and y, and δ that of Δ and z. Write $x=\Delta X$, $y=\Delta Y$, $\Delta=\delta D$, $z=\delta\zeta$. Then (1) becomes $\delta D^2(X^2-mY^2)=\zeta w$. The common factor δ of x, y, and z is prime to w, hence δ divides ζ. Since D^2 is prime to ζ, it divides w. Write $\zeta=\delta Z$, $w=D^2W$. Hence

$$(7)\qquad X^2-mY^2=ZW\qquad (X \text{ prime to } Y)\ .$$

For this case we shall prove that $X, \ldots, W$ have the values stated for $x/\rho, \ldots, w/\rho$ in the theorem. But

$$(8)\qquad x=\delta DX\ ,\quad y=\delta DY\ ,\quad z=\delta^2 Z\ ,\quad w=D^2W\ .$$

In the resulting expressions we replace $\delta\xi$ by ξ, $\delta\eta$ by η, Du by u, and Dv by v, and obtain the values for $x/\rho, \ldots, w/\rho$ in the theorem. Hence it suffices to prove the theorem for the case in which x and y are relatively prime.

Then y is prime to w by (1). Hence there are solutions ϕ, ζ of $x=y\phi+w\zeta$. Insertion into (1) gives

$$(\phi^2-m)y^2+2w\phi y\zeta+w^2\zeta^2=zw\ .$$

Since all terms except the first are divisible by w, while y^2 is prime to w, we must have $\phi^2-m=\epsilon w$, where ϵ is an integer. Hence

$$z=\epsilon y^2+2\phi y\zeta+w\zeta^2\ ,$$

whence z is represented by a form (ϵ, ϕ, w) of determinant m. There is a linear transformation

$$(9) \qquad y=v\xi+u\eta\ , \quad \zeta=s\xi+t\eta\ , \quad vt-us=1\ ,$$

with integral coefficients, which replaces (ϵ, ϕ, w) by the representative form (2) of its class. Hence z is represented by $F(\xi, \eta)$. The inverse transformation

$$(10) \qquad \xi=ty-u\zeta\ , \quad \eta=-sy+v\zeta$$

replaces $F(\xi, \eta)$ by (ϵ, ϕ, w). By the coefficients of ζ^2, we get $F(-u, v)=w$.

Thus y, z, w have the values in Theorem 69 for $\rho=1$ The values of x may be computed by (1); or directly from (39) of § 53 if we replace a, b, c, r, s, v by $e, f, g, \xi, \eta, -v$, respectively.

This completes the proof of the theorem.

EXERCISES XXVI

1. For $m=-3$, the solutions are derived from (5) by replacing each 5 by 3.

2. Not all solutions (6) are included in (5). For $\rho=\xi=\eta=u=v=1$, (6) gives $x=1$ or -1, $z=7$. If these were of type (5) then $\rho=\pm 1$ and $\pm 7=\xi^2+5\eta^2$, which is impossible in integers

3. If we permit the interchange of z and w, we may choose the upper sign in x. Hint: Replace ξ, η, u, v by $u, -v, -\xi, \eta$, respectively.

4. If $m\equiv 1 \pmod 4$, all integral solutions of

$$x^2+xy+\tfrac{1}{4}(1-m)y^2=zw$$

are the products of an integer ρ by

$$x=e\xi u+f\eta u-(f+1)\xi v-g\eta v\ , \quad y=\xi v+\eta u\ ,$$
$$z=e\xi^2+(2f+1)\xi\eta+g\eta^2\ . \quad w=eu^2-(2f+1)uv+gv^2\ ,$$

where the form z is restricted to representative forms, one from each class of discriminant m. If $m<0$, we may assume that these representative forms are positive and reduced For, the

solution is unaltered when we replace $\xi, \eta, e, g, f, u, v, \rho$ by $\eta, \xi, -g, -e, -f-1, -v, -u, -\rho$, respectively.

5. In Ex. 4 we may take $e=g=1, f=0$ if $m=-3$; $e=1, f=0$, $g=2$, 3, or 5 if $m=-7, -11$, or -19, respectively. If $m=-15$, we may take z to be [1, 1, 4] or [2, 1, 2] and get two sets of solutions.

6. To solve $x^2+y^2+Z^2=W^2$ completely, take $z=W+Z$, $w=W-Z$, and apply (4). Since $z-w$ is even, the parameters are subject to the condition $\xi+\eta\equiv u+v \pmod 2$.

7. Similarly, solve $B+Z^2=W^2$, where B is either x^2-my^2 or the form in Ex. 4.

8. Solve $3x^2+5y^2=zw$. It suffices to take x prime to y. Write $X=3x$, $W=3w$. Then $X^2+15y^2=zW$. We apply Theorem 69 with the upper sign in x. Since ρ divides $X=3x$ and y, ρ divides 3. When $\rho=1$, and $F=3\xi^2+5\eta^2$, we have

$$3x=3\xi u-5\eta v\ , \quad y=\xi v+\eta u\ , \quad z=3\xi^2+5\eta^2\ , \quad 3w=3u^2+5v^2\ .$$

Hence $v=3V$. Multiply the resulting values of $x, \ldots, w$ by an arbitrary integer ρ. Treat the remaining cases $F=\xi^2+15\eta^2$ and $\rho=3$.

58. Problem. Find all integral solutions of

$$(11) \qquad ax^2+bxy+cy^2=zw\ .$$

Any common divisor ω of a, b, c divides zw. Hence we may write $z=\rho Z$, $w=\sigma W$, where $\rho\sigma=\omega$, and obtain an equation of type (11) in which a, b, c now have no common factor >1. It is known that $ax^2+\ldots$ represents an infinitude of primes and hence is equivalent to a form whose first coefficient is a prime. Hence let a be a prime. As in § 57, we may assume that x and y are relatively prime. We may multiply (11) by $4a$, complete the square on x, and proceed* as in Ex. 8.

We may improve on this method by using

* The author treated the general equation (11) by this method in *Bull. Amer. Math. Soc.*, XXXII (1926), 644–48

THEOREM 70. *If a number is represented properly by a form* [a, b, c] *of discriminant* d, *then any divisor of that number is represented by some form of the same discriminant* d.

Let G be the g.c.d. of y and w. In (11), G divides ax^2. Since x and y are relatively prime, G divides a. Then

$$y=G\omega, \quad w=Gk\ , \quad a=Gh\ , \quad hx^2+bx\omega+cG\omega^2=zk\ .$$

Since ω and k are relatively prime there exist solutions θ and ζ of $x=\omega\theta+k\zeta$. Elimination of x gives

$$\alpha\omega^2+\phi k\omega\zeta+hk^2\zeta^2=zk\ , \quad \alpha=h\theta^2+b\theta+cG\ , \quad \phi=b+2h\theta\ .$$

Hence $\alpha\omega^2$ is divisible by k. The same is true of α. Write $\alpha=k\epsilon$, $\gamma=hk$. Thus

$$z=\epsilon\omega^2+\phi\omega\zeta+\gamma\zeta^2\ .$$

The discriminant of this form is equal to that of (11).

Let this form z become a representative form $F(\xi, \eta)$ by a transformation (9) with ω in place of y. As with (10), we get $\gamma=F(-u, v)$.

THEOREM 71. *All integral solutions of* (11) *are the products of the same arbitrary integer* ρ *by* x, y, z, w, *where*

(12) $$z=e\xi^2+f\xi\eta+g\eta^2\ , \quad y=G(v\xi+u\eta)\ ,$$
$$aw, G^2=eu^2-fuv+gv^2\ .$$

Here G *divides* a. *We may find* x *from* (11).

EXERCISES XXVII

1. Solve $3x^2+5y^2=zw$ by the last method. It suffices to take x prime to y. Here $G=1$ or 3. If $G=3$, (12) give integral values to z, y, w. Next, let $G=1$. First, let $F=(3, 0, 5)$. Then $3w=3u^2+5v^2$, $v=3V$. Hence

$$z=3\xi^2+5\eta^2\ , \quad y=3V\xi+u\eta\ , \quad w=u^2+15V^2\ .$$

The proposed equation gives $\pm x=u\xi-5V\eta$. But if $F=(1, 0, 15)$, then

$$z=\xi^2+15\eta^2\ , \quad y=v\xi+3U\eta\ . \quad w=3U^2+5v^2 \quad \pm x=U\xi-5v\eta\ .$$

2. Solve $3x^2+4y^2=zw$.

3. Every divisor of a sum of two relatively prime squares is a sum of two squares. There exist infinitely primes $4n+1$. Hint: If p were the largest such prime, use π^2+1, where π is the product of all the primes $\leqq p$.

4. Every odd divisor of x^2+3y^2 (x and y relatively prime) is of that form. There exist infinitely many primes $6n+1$. Use $3\pi^2+1$.

5. There exist infinitely primes $8n+5$. Use $(3\cdot 5\cdot 7\cdots p)^2+4$.

6. Solve $ax^2+bxy+cy^2=vw_1w_2$. Write $z=w_1w_2$ and employ all solutions of (11). Then $z=\rho Q$, $Q=e\xi^2+f\xi\eta+g\eta^2$. Since ρ divides w_1w_2, we may write $\rho=h_1h_2$, $w_i=h_iW_i$. Then $Q=W_1W_2$, which is an equation of type (11).

7. Hence solve $x^2+y^2=uvw$.

8. Solve $x^2+y^2=zuvw$.

59. Method of Euler and Lagrange. In his *Algebra* of 1770, Euler obtained integral solutions of

$$ax^2-my^2=z^3 \tag{13}$$

by writing A and M for the square roots of a and m and assuming that

$$Ax+My=(Au+Mv)^3\ , \tag{14}$$

and the like equation with M replaced by $-M$. We get

$$x=au^3+3muv^2\ ,\quad y=3au^2v+mv^3\ ,\quad z=au^2-mv^2 \tag{15}$$

But he noted that this method evidently fails to give integral solutions with $y=1$ when $a=2$, $m=5$, whereas $2x^2-5=z^3$ for $x=4$, $z=3$.

Lagrange extended this method in 1769 and later in 1774 in his addition to Euler's *Algebra* The function

$$\xi^2-m\eta^2=(\xi+M\eta)(\xi-M\eta)\ ,\quad M^2=m\ , \tag{16}$$

evidently has the property that its product by u^2-mv^2 is x^2-my^2, where

$$x+My=(\xi+M\eta)(u+Mv)\ , \tag{17}$$

whence

(18) $$x=\xi u+m\eta v\ ,\quad y=\xi v+\eta u\ .$$

Lagrange took $\xi=u$, $\eta=v$, and concluded that $x^2-my^2=z^2$ holds if $x=u^2+mv^2$, $y=2uv$, $z=u^2-mv^2$; then the factors in the second member of (17) are equal. Next, he took these values of x and y as new values of ξ and η:

$$\xi=u^2+mv^2\ ,\quad \eta=2uv\ ,\quad \xi+M\eta=(u+Mv)^2\ ,$$

and concluded that $x^2-my^2=z^3$ has the solutions (15) with $a=1$.

A repetition of this process evidently leads to (certain) solutions of $x^2-my^2=z^n$.

But this method rarely gives all integral solutions, even after inserting an arbitrary integral factor of proportionality. For example, by Lagrange's first remark, $x^2-my^2=zw$ has solutions given by (18) and $z=\xi^2-m\eta^2$, $w=u^2-mv^2$. For $m=-5$, these are essentially (5), while the further solutions (6) are not found in this way.

While this method fails to meet the modern requirement of finding all integral (or rational) solutions, it has the merit of yielding quickly an infinitude of them.

EXERCISES XXVIII

1. Generalize (16), etc., to $\xi^2+a\xi\eta+b\eta^2=(\xi+\alpha\eta)(\xi+\beta\eta)$, where α and β are the roots of $\alpha^2-a\alpha+b=0$.

2. Let α_1, α_2, α_3 be the roots of $\alpha^3-a\alpha^2+b\alpha-c=0$. Then

$$F(x,y,z)=\Pi(x+\alpha_i y+\alpha_i^2 z)=x^3+ax^2y+(a^2-2b)x^2z+bxy^2$$
$$+(ab-3c)xyz+(b^2-2ac)xz^2+cy^3+acy^2z+bcyz^2+c^2z^3$$

If $x+\alpha y+\alpha^2z=(\xi+\alpha\eta+\alpha^2\zeta)(u+\alpha v+\alpha^2 w)$, evidently $F(x,y,z)=F(\xi,\eta,\zeta)\,F(u,v,w)$. Taking $\xi=u$, $\eta=v$, $\zeta=w$, we see that $F=\sigma^2$ has the solutions

$$x=u^2+2cvw+acw^2\ ,\qquad y=2uv-2bvw+(c-ab)w^2$$
$$z=2uw+v^2+2avw+(a^2-b)w^2\qquad \sigma=F(u,v,w)$$

Show how to solve $F=\sigma^3$.

3. In Ex. 2 make $z=0$ by choice* of u in terms of v and w. Hence find solutions of $x^3+ax^2y+bxy^2+cy^3=\sigma^2$. For the case $a=b=0$, multiply x and y by w^2 and σ by w^3, and take $v=2V$. We get

$$x=4V(cw^3+V^3)\ ,\quad y=w(cw^3-8V^3)\ ,$$
$$\sigma=F(-2V^2\ ,\ 2Vw,\ w^2)=-8V^6+20cV^3w^3+c^2w^6\ .$$

4. Treat the case $a=b=0$ of Ex. 2 by determinants. Then

$$F=-\begin{vmatrix} x & \alpha y & \alpha^2 z \\ \alpha y & \alpha^2 z & x \\ \alpha^2 z & x & \alpha y \end{vmatrix}\ ,\qquad \alpha^3=c\ .$$

The product of two such determinants is one of the same type.

* Legendre took $v=(t-a)w,\ 2u=(b-t^2)w$.

CHAPTER VII

INDEFINITE BINARY QUADRATIC FORMS

Partly in view of the important applications to minima in chapter xi, we here develop the theory of reduction and equivalence for all real, indefinite forms. The methods and results are in marked contrast with those in chapter v for definite forms.

60. Relations between the roots of equivalent forms. In § 40, we saw that a real form

(1) $$q=[a,\ b,\ c]=ax^2+bxy+cy^2$$

having a positive *discriminant* $d=b^2-4ac$ takes both positive and negative values and hence is called an *indefinite* form. Let R denote the positive square root of d. Now $x-\omega y$ is a factor of q if and only if

(2) $$a\omega^2+b\omega+c=0\ .$$

Its *first* and *second* roots are respectively

(3) $$f=\frac{R-b}{2a}\ ,\qquad s=\frac{-R-b}{2a}\ .$$

We assume that $a\neq 0$ and that neither root is rational (this is true of every integral form with d not a square). Then the values of f, s, and R uniquely determine a, b, c.

THEOREM 72. *Let the integral transformation*

(4) $$x=\alpha X+\beta Y,\qquad y=\gamma X+\delta Y\ ,\qquad \alpha\delta-\beta\gamma=1$$

replace q *by* $Q=[A,\ B,\ C]$. *Then their first roots* f *and* F *and their second roots* s *and* S *are connected by the relations*

(5) $$f=\frac{\alpha F+\beta}{\gamma F+\delta}\ ,\qquad s=\frac{\alpha S+\beta}{\gamma S+\delta}\ ,\qquad \alpha\delta-\beta\gamma=1\ .$$

For, (4) replaces $x-\omega y$ by $t(X-\Omega Y)$, where $t=\alpha-\omega\gamma\neq 0$ and

$$\Omega=\frac{-\beta+\delta\omega}{\alpha-\gamma\omega}. \tag{6}$$

In (6) we replace ω by $(\pm R-b)/(2a)$ from (3) and get

$$\Omega=\frac{\pm\delta R-\delta b-2\beta a}{\mp\gamma R+\gamma b+2a\alpha}=\frac{-2aB\pm 2aR}{4aA}=\frac{\pm R-B}{2A},$$

by multiplying the numerator and denominator of the first fraction by $\pm\gamma R+\gamma b+2a\alpha$ and employing $\alpha\delta-\beta\gamma=1$ and the values of A and B in § 38. Hence $\Omega=F$ when $\omega=f$, and $\Omega=S$ when $\omega=s$. The theorem follows since the solved form of (6) is

$$\omega=\frac{\alpha\Omega+\beta}{\gamma\Omega+\delta}. \tag{7}$$

We next prove the converse theorem.

THEOREM 73. *If q and Q have the same discriminant d and if their roots are connected by relations (5), then transformation (4) replaces q by Q.*

For, let (4) replace q by T, whose first and second roots are ϕ and σ. By Theorem 72,

$$f=\frac{\alpha\phi+\beta}{\gamma\phi+\delta}, \qquad s=\frac{\alpha\sigma+\beta}{\gamma\sigma+\delta}.$$

Hence $\phi=F$, $\sigma=S$. We saw that the two roots and $R^2=d$ uniquely determine the form. Hence $T=Q$.

61. Reduced forms. The form q is called *reduced* if

$$|f|<1, \qquad |s|>1, \qquad fs<0. \tag{8}$$

Then, by (3), $R-b$ and $R+b$ are of like sign and the former is numerically less than the latter. Hence $0<b<R$, and

$$0<R-b<2|a|<R+b. \tag{9}$$

Conversely, (9) imply $b>0$ and (8). Hence $[a, b, c]$ *is reduced if and only if* (9) *hold.*

Note that f and a have the same sign, and c the opposite sign since $4ac=b^2-R^2<0$. In view of

$$(R-b)(R+b)=4\,|ac|\ ,$$

(9) are equivalent to the like inequalities with a replaced by c.

THEOREM 74. *If one of* $[a, b, c]$ *and* $[c, b, a]$ *is reduced, the other is reduced.*

THEOREM 75. *Every real form of discriminant* $d>0$ *is equivalent to a form* $[a, b, c]$ *in which*

$$(10) \qquad |b| \leqq |a| \leqq \sqrt{\tfrac{1}{3}d}$$

We first show how to secure the second inequality. If $|a| > \sqrt{\frac{1}{3}d}$ in a given $[a, b, c]$, we apply transformation

$$x=hX+Y,\ y=-X$$

of determinant unity and obtain $[A, B, a]$, where $B=2ah-b$. We can choose an integer h such that $|B| \leqq |a|$. Then

$$4Aa=B^2-d<B^2 \leqq a^2 \qquad -4Aa=d-B^2 \leqq d<3a^2$$

Hence $4\,|Aa| <3a^2$, $|A| < \frac{3}{4}|a|$.

If $|A| > \sqrt{\frac{1}{3}d}$, we repeat the discussion and obtain an equivalent form $[A_1, B_1, A]$ having $|A_1| < \frac{3}{4}|A| < (\frac{3}{4})^2|a|$.

Since $(\frac{3}{4})^n$ may be made as small as we please by taking n sufficiently large, we ultimately obtain an equivalent form $[a', b', c']$ in which $|a'| \leqq \sqrt{\frac{1}{3}d}$. Replacing x by $x+ky$ we obtain $[a', \beta, \gamma]$, where $\beta=b'+2ka'$. We can choose an integer k such that $|\beta| \leqq |a'|$. This proves Theorem 75.

THEOREM 76. *Every real form is equivalent to a reduced form.*

We may assume that $b^2 \leqq \frac{1}{3}d$ by (10); but we make use

only of $b^2 \leqq d$. Then $4|ac| = d - b^2 \leqq d$, whence not both $2|a|$ and $2|c|$ are $> R$. If necessary, we replace x by y and y by $-x$, and have $2|c| \leqq R$. Also, $c \neq 0$ since neither root of (2) is rational. By repeated duplications of the segment from $R - 2|c|$ to R, we obtain the complete line. Hence to any real b corresponds a real b' within our segment such that $b - b'$ is the product of $2|c|$ by an integer, whence $b - b' = 2kc$, where k is an integer. In $[a, b, c]$ replace y by $y - kx$. We get $[a', b', c] = \phi$. Since b' is in the segment,

$$0 \leqq R - b' \leqq 2|c| \leqq R + b'$$

If any of these signs were $=$, one of the roots of ϕ would be 0 or ± 1, whence a root of $[a, b, c]$ would be rational, contrary to hypothesis. Hence ϕ is a reduced form.

The process furnishes an integral transformation of determinant 1 which replaces the given form by a reduced form.

62. Chain of equivalent, reduced forms. Consider the following case of transformation (4) and (7):

$$(11) \qquad x = Y, \qquad y = -X + \delta Y; \qquad \frac{1}{\omega} = \delta - \Omega .$$

As in § 41, it replaces $q = [a, b, a_1]$ by the right neighboring form $r = [a_1, b_1, a_2]$, where

$$(12) \qquad b_1 = -b - 2\delta a_1 ,$$

and a_2 is then found from the discriminant.

THEOREM 77. *Every reduced form q has one and but one reduced, right neighboring form.*

Let f and s denote the first and second roots of q. Let $|\delta|$ denote the largest integer $< 1/|f|$, while δ has the same sign as f and a, and hence the opposite sign to a_1. By (8), $|\delta| > 0$. For this δ, (11) replaces q by r, whose first root is

$$(13) \qquad F = \delta - \frac{1}{f} .$$

Hence F is numerically <1 and has the opposite sign to δ and f. Since the sign of s is opposite to that of f and δ, the second root $S=\delta-1/s$ of r is of the same sign as δ and is numerically >1. Hence r is a reduced form by (8).

Moreover, r is reduced only when δ is chosen as indicated. For, if q and r are reduced, F has the same sign as a_1, and f has the sign opposite to a_1. Thus $|f|<1$, $|F|<1$, and (13) require that δ be of the same sign as f and that $|\delta|$ be the largest integer $<1/|f|$.

THEOREM 78. *Every reduced form has one and but one reduced, left neighboring form.*

For, if $[a, b, a_1]$ is reduced, also $[a_1, b, a]$ is reduced by Theorem 74. The latter has a unique reduced, right neighboring form $[a, l, m]$. Hence the reduced form $[m, l, a]$ has $[a, b, a_1]$ as a right neighboring form.

Let Φ_0 be any reduced form Let Φ_1 and Φ_{-1} be its unique reduced, right and left neighboring forms. In this manner we obtain a *chain*

$$(14) \qquad \ldots, \Phi_{-2}, \Phi_{-1}, \Phi_0, \Phi_1, \Phi_2, \ldots$$

of equivalent, reduced forms.

63. Determination of reduced, integral forms.

THEOREM 79. *There is only a finite number of reduced integral forms of a given discriminant $d>0$.*

By (9), $0<b<R$. Also, b is even or odd, according as $d\equiv 0$ or 1 (mod 4). For each such integer b, we express the integer $\frac{1}{4}(d-b^2)=|ac|$ in all ways as a product of two positive integers which lie between $\frac{1}{2}(R-b)$ and $\frac{1}{2}(R+b)$ and prefix opposite signs to the factors

For example, if $d=12$, then $b=2$, $|ac|=2$ The four reduced forms lie in two chains $\Phi_0=[1, 2, -2]$, $\Phi_1=[-2, 2, 1]$, and $[-1, 2, 2]$, $[2, 2, -1]$. According as $\delta=1$ or -2, transformation (11) replaces Φ_0 by Φ_1 or Φ_1 by Φ_0

If $d=17$, either $b=1$, $|a|=|c|=2$, or $b=3$ and one of $|a|$

and $|c|$ is 1 and the other is 2. The six reduced forms lie in one chain: $\Phi_0=[1, 3, -2]$, $\Phi_1=[-2, 1, 2]$, $\Phi_2=[2, 3, -1]$, $\Phi_3=[-1, 3, 2]$, $\Phi_4=[2, 1, -2]$, $\Phi_5=[-2, 3, 1]$. The successive values of δ are $1, -1, 3, -1, 1, -3$. Transformation (11) with $\delta=-3$ replaces Φ_5 by Φ_0.

64. Periods. For integral forms, the members of a chain (14) are not all distinct. The first coefficients of adjacent forms have opposite signs. Let therefore $\Phi_k\equiv\Phi_{k+2n}$. Their left neighboring forms are identical, etc., whence $\Phi_0\equiv\Phi_{2n}$. Hence every form in the chain is identical with one of $\Phi_0, \ldots, \Phi_{2n-1}$. These will be distinct if n is chosen so that Φ_0 is distinct from the others. Then these $2n$ forms are said to form a *period*.

EXERCISES XXIX

Find all periods as follows.

1. $d=5$, $[1, 1, -1]$, $[-1, 1, 1]$.
2. $d=8$, $[1, 2, -1]$, $[-1, 2, 1]$.
3. $d=13$, $[1, 3, -1]$, $[-1, 3, 1]$.
4. $d=20$, $[1, 4, -1]$, $[-1, 4, 1]$; and $[2, 2, -2]$, $[-2, 2, 2]$.
5. $d=21$, $[1, 3, -3]$, $[-3, 3, 1]$, and $[-1, 3, 3]$, $[3, 3, -1]$.
6. $d=24$, $[1, 4, -2]$, $[-2, 4, 1]$, and $[-1, 4, 2]$, $[2, 4, -1]$.
7. $d=52$, $[3, 2, -4]$, $[-4, 6, 1]$, $[1, 6, -4]$, $[-4, 2, 3]$, $[3, 4, -3]$, $[-3, 2, 4]$, $[4, 6, -1]$, $[-1, 6, 4]$, $[4, 2, -3]$, $[-3, 4, 3]$; and $[2, 6, -2]$, $[-2, 6, 2]$. For the period of ten, the δ's are $1, -6, 1, -1, 1, -1, 6, -1, 1, -1$.
8. $d=221$, $[5, 11, -5]$, $[-5, 9, 7]$, $[7, 5, -7]$, $[-7, 9, 5]$, and $[1, 13, -13]$, $[-13, 13, 1]$; and two periods derived from these by changing the signs of all extreme coefficients.

65. Notations. It is convenient to write

$$\Phi_i=[(-1)^i A_i,\ B_i,\ (-1)^{i+1}A_{i+1}]\,. \tag{15}$$

Let transformation (11) with $\delta=\delta_i$ replace Φ_i by Φ_{i+1}. By (12),

$$B_i+B_{i+1}=2g_iA_{i+1}\,,\qquad g_i=(-1)^i\delta_i\,. \tag{16}$$

Since the chain (14) is determined by any one of its members, we may choose Φ_0 so that A_0 is positive. Then A_i, B_i, g_i are positive for every i. If f_i and s_i are the first and second roots of Φ_i, write

$$(17)\qquad F_i=\frac{(-1)^i}{f_i}\qquad S_i=\frac{(-1)^{i+1}}{s_i}\,.$$

Since the discriminant of (15) is $d=R^2$,

$$(18)\quad F_i=\frac{R+B_i}{2A_{i+1}}\,,\quad S_i=\frac{R-B_i}{2A_{i+1}}\quad F_i>1\,,\quad 0<S_i<1$$

By (11), $1/f_i=\delta_i-f_{i+1}$ and similarly with s instead of f. Multiplication by $(-1)^i$ gives

$$(19)\qquad F_i=g_i+\frac{1}{F_{i+1}}\qquad \frac{1}{S_i}=g_{i-1}+S_{i-1}\,,$$

after the subscripts in the second are reduced by 1

For the example $d=12$ in § 63, $g_0=1$, $g_1=2$, $\Phi_2=\Phi_0$, whence

$$F_0=1+\frac{1}{F_1},\qquad F_1=2+\frac{1}{F_2},\qquad F_2=F_0,\qquad F_0=1+\cfrac{1}{2+\cfrac{1}{F_0}}$$

Hence we have a development of F_0 into a periodic continued fraction, as will be explained next.

66. Continued fractions. For $p>0$ let

$$p=q_1+\frac{1}{p_1}\,,\qquad p_1=q_2+\frac{1}{p_2}\,,\qquad p_2=q_3+\frac{1}{p_3}\,,\ \ldots\,,$$

where q_1, q_2, q_3, ... are the largest integers $\leqq p$, $\leqq p_1$, $\leqq p_2$, ..., respectively. While q_1 may be zero, q_2, q_3, ... are all $\geqq 1$. In case $q_k=p_{k-1}$, the equations stop with the

kth. In any case, p is said to have the following development into a continued fraction:

$$p=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\ldots}},$$

which is denoted by $(q_1, q_2, q_3, \ldots)$.

The first three *convergents* to p are defined to be

$$\frac{q_1}{1}, \qquad q_1+\frac{1}{q_2}=\frac{1+q_1q_2}{q_2}, \qquad \frac{(1+q_1q_2)q_3+q_1}{q_2q_3+1},$$

where the third was derived from the second by replacing q_2 by q_2+1/q_3. Similarly, we define the successive convergents by the property that the $(r+1)$th convergent is derived from the rth convergent by replacing q_r by q_r+1/q_{r+1}.

THEOREM 80. *The kth convergent to* $(q_1, q_2, \ldots)$ *is the quotient* n_k/d_k *of*

$$(20) \qquad n_k=n_{k-1}q_k+n_{k-2}, \qquad d_k=d_{k-1}q_k+d_{k-2}.$$

This is seen to be true when $k=3$ if we take

$$(21) \quad n_1=q_1, \qquad d_1=1, \qquad n_2=1+q_1q_2, \qquad d_2=q_2.$$

Let the rth convergent be the quotient of the values (20) for $k=r$. Then the foregoing property gives for the $(r+1)$th convergent the value

$$\frac{n_{r-1}(q_r+1/q_{r+1})+n_{r-2}}{d_{r-1}(q_r+1/q_{r+1})+d_{r-2}}=\frac{n_r+n_{r-1}/q_{r+1}}{d_r+d_{r-1}/q_{r+1}},$$

where the equality follows from (20) with $k=r$. The final fraction is seen to be the quotient of the numbers (20) for $k=r+1$. This completes the proof by induction. Expressed otherwise, the numbers n_k, $d_k (k=1, 2, 3, \ldots)$ defined by (20) and (21) are such that n_k/d_k is the kth convergent to $(q_1, q_2, \ldots)$.

Multiply equations (20) by d_{k-1} and $-n_{k-1}$, respectively, and add. We get

$$n_k d_{k-1} - d_k n_{k-1} = -(n_{k-1} d_{k-2} - d_{k-1} n_{k-2}) .$$

Hence the product of the left member by $(-1)^k$ is unaltered when k is replaced by $k-1$ and hence its value is independent of k. For $k=2$, it is $(1+q_1q_2)-q_2q_1=1$. This proves

THEOREM 81. *For the numbers defined by* (20) *and* (21),

$$(22) \qquad n_k d_{k-1} - d_k n_{k-1} = (-1)^k .$$

Since n_k and d_k are therefore relatively prime, the fraction n_k/d_k computed by means of (20) is irreducible.

Consider $p=(q_1, q_2, \ldots)=(q_1, \ldots, q_{k-1}, q)$, where therefore $q=(q_k, q_{k+1}, \ldots)$. Replace q_k by Q_k and write Q for $(Q_k, q_{k+1}, \ldots)$. Hence $P=(q_1, \ldots, q_{k-1}, Q)$ is derived from p by replacing q_k by Q_k. By (20),

$$p=\frac{N}{D}, \qquad N=n_{k-1}q+n_{k-2}, \qquad D=d_{k-1}q+d_{k-2}.$$

Hence

$$P=\frac{n_{k-1}Q+n_{k-2}}{d_{k-1}Q+d_{k-2}}.$$

We find that $P<p$ if $mQ<mq$, where

$$m=d_{k-2}n_{k-1}-n_{k-2}d_{k-1}=(-1)^{k-1},$$

by (22). If k is odd, the condition is therefore $Q<q$, which is equivalent to $Q_k<q_k$. But if k is even, the condition is $Q>q$ or $Q_k>q_k$.

THEOREM 82. *If in $p=(q_1, q_2, \ldots)$ we decrease q_k, the value of p is decreased when k is odd, but increased when k is even. If we increase q_k, the value of p is increased when k is odd, but decreased when k is even*

THEOREM 83. *If* $(q_1, \ldots, q_r)$ *has the kth convergent* n_k/d_k *for* $k=1, \ldots, r$, *then*

$$\frac{n_r}{n_{r-1}}=(q_r, q_{r-1}, \ldots, q_2, q_1), \qquad \frac{d_r}{d_{r-1}}=(q_r, \ldots, q_2).$$

For, by (20),

$$\frac{n_k}{n_{k-1}}=q_k+\frac{1}{n_{k-1}/n_{k-2}}, \qquad \frac{d_k}{d_{k-1}}=q_k+\frac{1}{d_{k-1}/d_{k-2}}.$$

We use this for $k=r, r-1, \ldots, 3$, but use

$$\frac{n_2}{n_1}=q_2+\frac{1}{q_1}, \qquad \frac{d_2}{d_1}=q_2$$

which follow from (21). Hence the theorem is true.

From (19) we have at once

$$(23) \qquad F_i=(q_i, q_{i+1}, q_{i+2}, \ldots), \qquad S_i=(0, q_{i-1}, q_{i-2}, \ldots)$$

whence

$$(24) \qquad \frac{1}{f_0}=F_0=(q_0, q_1, \ldots, q_{i-1}, F_i).$$

$$(-1)^{i+1}s_i=\frac{1}{S_i}=\left(q_{i-1}, q_{i-2}, \ldots, q_0, \frac{1}{S_0}\right)$$

For the example with $d=17$ in § 63, we have $F_0=(1, 1, 3, F_3)$, whence the triple 1, 1, 3 is repeated periodically. We use the notation $F_0=(\dot{1}, 1, \dot{3})$. This result may be verified by converting $1/f_0=\frac{1}{4}(\sqrt{17}+3)$ into a continued fraction.

67. Equivalent, reduced forms.

THEOREM 84. *Two equivalent, reduced forms of the same positive discriminant d belong to the same chain.*

It suffices to prove this when either form is replaced by its right neighboring form. Hence let q and Q be two distinct equivalent, reduced forms whose first coefficients are positive. Then their first roots f and F are positive and

<1, while their second roots s and S are negative and numerically >1. Let T be a transformation (4) with integral coefficients of determinant 1 which replaces q by Q. Hence their roots satisfy relations (5). Since we may change the signs of the four coefficients of T, we may assume that either $\alpha>0$, or $\alpha=0$, $\gamma>0$.

If $\alpha=0$, then $\gamma=1$, $\beta=-1$, and, by (5),

$$-\delta=F+\frac{1}{f}>1\ , \qquad \delta=-S-\frac{1}{s}>1\ ,$$

a contradiction. Hence $\alpha\geqq 1$. By (5),

$$(25)\qquad \frac{1}{f}=\frac{\gamma+\delta/F}{\alpha+\beta/F}\ , \qquad \frac{1}{s}=\frac{\gamma+\delta/S}{\alpha+\beta/S}\ , \qquad \alpha\delta-\beta\gamma=1\ .$$

Hence

$$(26)\qquad \left(\frac{\alpha}{f}-\gamma\right)(\alpha F+\beta)=1\ , \qquad \left(\frac{\alpha}{s}-\gamma\right)(\alpha S+\beta)=1\ .$$

If $\beta=0$, then $\alpha=\delta=1$ and (26_2) gives

$$\gamma=\frac{1}{s}-\frac{1}{S}<\frac{-1}{S}<1\ , \qquad -\gamma<\frac{-1}{s}<1\ , \qquad |\gamma|<1\ , \qquad \gamma=0$$

If $\gamma=0$, then $\alpha=\delta=1$ and (26_1) gives $\beta=f-F$, $|\beta|<1$, $\beta=0$. In both cases, T is the identity transformation and $q=Q$, contrary to hypothesis. Hence $\beta\gamma\neq 0$.

If $\beta>0$, then $\alpha F+\beta>1$, $\alpha/f-\gamma<1$, $\gamma+1>\alpha/f>\alpha$, $\gamma\geqq\alpha$. If $\gamma>0$, then $\alpha/s-\gamma<-1$, $0>\alpha S+\beta>-1$, $\beta+1>-\alpha S>\alpha$, $\beta\geqq\alpha$. These prove that if $\gamma<0$, then $\beta<0$, and conversely. Hence $\beta\gamma>0$. Then $\alpha\delta=\beta\gamma+1>1$, $\delta>0$.

If β and γ are negative, we employ the inverse of T, which replaces Q by q. Hence after interchanging q and Q if necessary, we may assume that α, β, γ, δ are all positive. Thus $\gamma\geqq\alpha$, $\beta\geqq\alpha$,

$$\delta\beta\geqq\alpha\delta>\beta\gamma\ , \qquad \delta>\gamma; \qquad \delta\gamma\geqq\alpha\delta>\beta\gamma, \qquad \delta>\beta\ .$$

Hence α and γ give a solution of $\delta x-\beta y=1$ in positive integers x, y such that $x\leqq\beta$, $y<\delta$. From $\delta(x-\alpha)=\beta(y-\gamma)$ and the fact that δ, β are relatively prime, we have $x-\alpha=\beta m$, $y-\gamma=\delta m$, where m is an integer. But $x-\alpha$ is numerically $<\beta$. Hence $x-\alpha=0$, $y-\gamma=0$. The unique solution may be found as follows. We develop δ/β into a continued fraction $(g_0, g_1, \ldots, g_{i-1})$, where each $g\geqq 1$. We may assume that i is even. For, if i is odd and the continued fraction terminates with $u+1/v$, we replace this by the single term $u+1$ if $v=1$, but by

$$u+\frac{1}{(v-1)+1/1}\qquad \text{if } v>1\,.$$

Let y/x be the $(i-1)$th convergent. Since δ/β is the ith convergent, (22) for $k=i$ gives $\delta x-\beta y=(-1)^i=1$. By (20) and $q_k\geqq 1$, $n_k>n_{k-1}$, $d_k\geqq d_{k-1}$, viz., $\delta>y$, $\beta\geqq x$. We saw that the unique solution is $x=\alpha$, $y=\gamma$. Hence

$$\frac{\gamma}{\alpha}=(g_0, g_1, \ldots, g_{i-2})\,.$$

By (20) with $k=i+1$, we have

$$\left(g_0, g_1, \ldots, g_{i-2}, g_{i-1}, \frac{1}{F}\right)=\frac{\delta/F+\gamma}{\beta/F+\alpha}\,,$$

which is $1/f$ by (25). Since $1/F>1$, this is the continued fraction for $1/f$ up to the term g_{i-1}. But the development of $1/f$ into a continued fraction is unique. Hence if we write f_0 for f, we see from (24) that $1/F=F_i$, whence $F=(-1)^i f_i=f_i$ by (17). Here f_i is the first root of Φ_i in the chain containing $\Phi_0=q$.

It remains to prove that the second root s_i of Φ_i is equal to S. We apply Theorem 83 to $\delta/\beta=(g_0, \ldots, g_{i-1})$, whose $(i-1)$th convergent is γ/α, and conclude that

$$\frac{\delta}{\gamma}=(g_{i-1}, g_{i-2}, \ldots, g_0),\qquad \frac{\beta}{\alpha}=(g_{i-1}, \ldots, g_1)\,.$$

By (20) with $k=i+1$, we get

$$(g_{i-1}, g_{i-2}, \ldots, g_1, g_0, -s) = \frac{-s\delta+\beta}{-s\gamma+\alpha},$$

which is $-S$ by the solved form of (5_2). Since $1/S_0 = -s_0 > 1$, we see by writing s_0 for s, and, using (24_2), that $-s_i = -S$.

Since Q and Φ_i have the same first roots, same second roots, and same discriminant, they are identical.

68. Lower bound of numbers represented by a form.

THEOREM 85 (Lagrange). *If the forms $[a_i, b_i, a_{i+1}]$ constitute a chain of reduced forms of discriminant $d=R^2$, the a_i include all numbers numerically $<\frac{1}{2}R$ which are represented properly by a form in the chain.*

Let a be represented properly by such a form. There is an equivalent form $[a, B, C]$ with the first coefficient a. As in the proof of Theorem 76, we can determine b between $R-2|a|$ and R such that $b-B$ is the product of $2|a|$ by an integer. Hence $[a, B, C]$ is parallel to $f=[a, b, c]$. Since $2|a|<R$, f is a reduced form by (9). Hence a occurs among the a_i.

THEOREM 86. *The lower bound of the absolute values of the numbers represented by f for integers x and y, not both zero, is the lower bound of the $|a_i|$ of the chain of reduced forms equivalent to f.*

For, in a reduced $[a, b, c]$, $b>0$, $R^2=b^2-4ac$, $ac<0$ whence $4|ac|<R^2$, and the lesser of $|a|$ and $|c|$ is $<\frac{1}{2}R$ Hence f represents properly an integer numerically $<\frac{1}{2}R$. Our theorem now follows from Theorem 85.

69. Automorphs. Let $q=[a, b, c]$ be a primitive, integral form of discriminant $d>0$. Let (4) transform q into itself. By (5),

$$\omega = \frac{\alpha\omega+\beta}{\gamma\omega+\delta}, \qquad \gamma\omega^2+(\delta-\alpha)\omega-\beta=0$$

holds for each root of q. Hence its coefficients are proportional to those of (2): $\gamma=au$, $\delta-\alpha=bu$, $\beta=-cu$. Unless u is an integer its denominator contains a factor >1 which divides a, b, c, whereas q is primitive. Write t for $\alpha+\delta$. Then

$$\alpha\delta=\beta\gamma+1=1-acu^2\ ,\ t^2=(\delta-\alpha)^2+4\alpha\delta=4+du^2\ .$$

THEOREM 87. *Every automorph* $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ *of a primitive, integral form* $[a, b, c]$ *of discriminant* $d>0$ *has*

$$\alpha=\tfrac{1}{2}(t-bu)\ ,\ \beta=-cu\ ,\ \gamma=au\ ,\ \delta=\tfrac{1}{2}(t+bu)\ , \tag{27}$$

where t and u are integral solutions of

$$t^2-du^2=4\ . \tag{28}$$

Conversely, if t and u are integral solutions of (28), *the numbers* (27) *are integers and define an automorph.*

It remains to prove the converse. Since 2α and 2δ are integers whose sum is the even integer $2t$, they are both even or both odd. But

$$\alpha\delta=\tfrac{1}{4}(t^2-b^2u^2)=1-acu^2$$

is an integer. Hence 2α and 2δ are both even.

Let A denote transformation (4) for the values (27). That A is an automorph of q will follow from the canonical form which A takes when it is expressed in terms of new variables which are the factors of q:

$$\xi=w+Ry,\ \eta=w-Ry\quad (w=2ax+by\ ,\ R=\sqrt{d}). \tag{29}$$

Write W for $2aX+bY$. Then

$$2y=uW+tY\ ,\ 2w=tW+duY\ .$$

Analogous to (29), write $\xi'=W+RY$, $\eta'=W-RY$. Then A takes the canonical form

$$\xi=\tfrac{1}{2}(t+Ru)\xi'\ ,\quad \eta=\tfrac{1}{2}(t-Ru)\eta'\ . \tag{30}$$

By (28) this leaves $\xi\eta=4aq$ unaltered. Hence A is an automorph of q.

70. All integral solutions of (28).

THEOREM 88. *Equation* (28) *has a solution with* $u\neq 0$.

We employ a primitive, integral, reduced form Φ_0 whose first coefficient is positive. Let $2n$ be the number of forms in its period (§ 64); let f be its first root. By (24)

$$\frac{1}{f}=(\dot{g}_0,\ g_1,\ \ldots,\ \dot{g}_{2n-1})\ .$$

Let γ/α and δ/β denote its $(2n-1)$th and $2n$th convergents Since

$$\frac{1}{f}=\left(g_0,\ \ldots,\ g_{2n-1},\ \frac{1}{f}\right),$$

we see by (20) and (22) that

$$\frac{1}{f}=\frac{\delta f+\gamma}{\beta f+\alpha}\ ,\qquad f=\frac{\alpha f+\beta}{\gamma f+\delta}\qquad \alpha\delta-\beta\gamma=1\ .$$

Hence $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ is an automorph of Φ_0. Then by (27) we obtain a solution t, $u\neq 0$ of (28).

For our example with $d=17$ in § 63, $\gamma/\alpha=(1,1,3,1,1)$, $\gamma=16=u$, $9=\alpha=\frac{1}{2}(t-3u)$, $t=66$.

We proved that (28) has a solution $t\neq 0$, $u\neq 0$. Then t, $\pm u$, and $-t$, $\pm u$ are solutions. It therefore suffices to find the positive solutions If t, u and t', u' are two such sets, and $t'>t$, then $u'>u$. Hence there exists a set of integral solutions $T>0$, $U>0$, such that if t, u is any further positive solution, then $t>T$, $u>U$. We shall call (T, U) the *least positive solution* Write

$$\epsilon=\tfrac{1}{2}(T+RU)\ , \tag{31}$$

and let E be the automorph given by T, U. By (30), E^n is an automorph given by positive integers t_n, u_n defined by

$$\tfrac{1}{2}(t_n+Ru_n)=\epsilon^n .$$

Every positive solution (t, u) is one of these (t_n, u_n). If this were false, there would exist an integer $n \geqq 1$ such that

$$\epsilon^n < \tfrac{1}{2}(t+Ru) < \epsilon^{n+1} , \tag{32}$$

since $\epsilon > 1$. If (t, u) gives the automorph A, then in

$$\tfrac{1}{2}(t+Ru) \cdot \tfrac{1}{2}(t_n - Ru_n) = \tfrac{1}{2}(t'+Ru') ,$$

t', u' give the automorph AE^{-n} and hence are integers. Multiply (32) by $1/\epsilon^n = \tfrac{1}{2}(t_n - Ru_n)$. We get

$$1 < \tfrac{1}{2}(t'+Ru') < \epsilon .$$

By the first inequality and (28) in accents, we get

$$\tfrac{1}{2}(t'+Ru')\cdot\tfrac{1}{2}(t'-Ru')=1 , \quad 0 < \tfrac{1}{2}(t'-Ru') < 1 ,$$

whence t' and u' are positive. Hence $t' \geqq T$ and $u' \geqq U$, and $\tfrac{1}{2}(t'+Ru') \geqq \epsilon$, contrary to our second inequality.

THEOREM 89. *For $d>0$, all sets of integral solutions t, u of* (28) *are given by*

$$\tfrac{1}{2}(t+Ru) = \pm[\tfrac{1}{2}(T+RU)]^k \qquad (k=0,\ \pm 1,\ \pm 2, \ldots) ,$$

where T, U give the least positive solution, and $R=\sqrt{d}$.

EXERCISES XXX

1. There is a period of two reduced forms having $a=1$ in Φ_0 if and only if $d=\delta^2C^2+4C$ holds for positive integers δ, C. Then $\Phi_0=[1,\ \delta C,\ -C]$, $\Phi_1=[-C,\ \delta C,\ 1]$, and (28) has the solution $t=2+\delta^2C$, $u=\delta$. Apply to $d=5$, 8, 12, 13, 20, 21, 24, 221 (Ex. XXIX).

2. Show that Theorem 87 holds also if $d<0$ Hint Equate the two forms in Theorem 68, and obtain $\alpha a+b\gamma=\delta a$, $c\gamma=-\beta a$.

3. Solve (28) when $d<0$. If $-d>4$, $t=\pm 2$, $u=0$. If $-d=4$, the further solutions are $t=0$, $u=\pm 1$. If $-d=3$, the six solutions are $(t, u)=(\pm 2, 0), (\pm 1, 1), (\pm 1, -1)$.

4. Let d be positive or negative. If E is the automorph given by T, U, and if B is the automorph $\xi=-\xi'$, $\eta=-\eta'$ given by $t=-2$, $u=0$, all automorphs are given by E^k, E^kB $(k=0, \pm 1, \pm 2, \ldots)$. If $d<0$, B and hence all automorphs are powers of E.

5. Deduce the theory of Pell's equation $w^2-Du^2=1$ by taking $d=4D$.

71. Proper representations. The theory in § 46 holds for any d. When $d>0$, we now know how to find the infinitely many automorphs.

For example, let $d=8$. Then $N^2\equiv 2 \pmod{m}$ requires that each prime factor >2 of m be $\equiv \pm 1 \pmod 8$ and that m be not divisible by 4. If there are r distinct such prime factors, there are exactly 2^r roots. For a chosen root N, determine l by $N^2-ml=2$. Then $Q=[m, 2N, l]$ has discriminant 8 and hence is equivalent to $q=x^2-2y^2$, since there is a single period. Let T replace q by Q, and let A be the general automorph of q. Then AT and no further transformations replace q by Q. The coefficients in the first columns of the matrices of AT give all proper representations of m by q which belong to this root N. There are 2^r such formulas giving all proper representations of m by q. In particular, every prime $8k\pm 1$ is represented by both x^2-2y^2 and $2x^2-y^2$.

EXERCISES XXXI

1. For $m=7\cdot 17$ the roots are ± 11, ± 45: $T=\begin{pmatrix}\pm 11 & 1\\ -1, & 0\end{pmatrix}$, $\begin{pmatrix}13, & \pm 5\\ \pm 5, & 2\end{pmatrix}$, respectively. All proper representations x, y of 119 by x^2-2y^2 are

$$\pm 11w-2u,\quad -w\pm 11u; \qquad 13w\pm 10u,\quad \pm 5w+13u\,,$$

where $w^2-2u^2=1$.

2. The odd numbers represented properly by x^2-5y^2 are the products of primes $\equiv \pm 1 \pmod 5$ and 5. All proper representations of 11 are $x = \pm 4w - 5u$, $y = w \mp 4u$, with $w^2 - 5u^2 = 1$.

FIND ALL PROPER REPRESENTATIONS

3. Of 13 by x^2-3y^2.
4. Of 43 by x^2-6y^2.
5. Of 23 by x^2-13y^2.

72. Indefinite, ambiguous forms.

THEOREM 90. *Every integral, indefinite form f which is improperly equivalent to itself is equivalent to an ambiguous form. Every period which contains an ambiguous form contains exactly two ambiguous forms.*

Without loss of generality, let $f=[a, b, a_1]$ be reduced Since f is improperly equivalent to itself, it is equivalent to its *associate* $\phi=[a_1, b, a]$. By Theorem 74, ϕ is reduced and hence is in the period of f. If the reduced, right neighboring form to f is $f_1=[a_1, b_1, a_2]$, the associate $\phi_1=[a_2, b_1, a_1]$ of f_1 is the reduced, left neighboring form to ϕ. Similarly, if the reduced, right neighboring form to f_1 is f_2, the associate ϕ_2 of f_2 is the reduced, left neighboring form to ϕ_1. Proceeding in this way forward from f and backward from ϕ, we come ultimately to a pair of associates $[A, B, C]$ and $[C, B, A]$ which are neighboring forms in the period. Hence $B+B\equiv 0 \pmod{2C}$ and $[C, B, A]$ is an ambiguous form.

Similarly, by going backward from f and forward from ϕ, we reach ultimately a pair of neighboring forms, one of which is ambiguous.

Conversely, if a period contains an ambiguous form $[C, B, A]$, its left neighboring form is its associate.

CHAPTER VIII

SOLUTION OF $ax^2+by^2+cz^2=0$ IN INTEGERS

73. Introduction. This equation has had a long history and is of especial importance in the theory of numbers Although it was treated in §§ 29–31, we there assumed that it has a known solution. We shall here establish necessary and sufficient conditions for the existence of integral solutions and then show how to find all solutions. For later, important, applications we require a knowledge of the solutions in which x, y, z are relatively prime in pairs, and among them the solutions which satisfy certain congruences. To obtain all these results it is necessary to go deeply into the theory of this classic equation.

74. Theorem 91. *Under the following assumptions:*

(1) *The coefficients are relatively prime in pairs, are not all of the same sign, and no one is zero;*

(2) *No coefficient has a square factor* >1;

(3) $$ax^2+by^2+cz^2=0$$

has integral solutions, not all zero, if and only if

(4) $-bc$, $-ca$, $-ab$ *are quadratic residues of* a, b, c, *respectively.**

* First stated and proved by Legendre, *Mém Acad Sc Paris* (1785), pp 507–13; *Théorie des nombres* (1798), pp 43–50, *ibid* (2d ed 1808), pp 35 41; *ibid* (3d ed, 1830) I, pp 41–48 A proof by means of quadratic forms in three variables was given by Gauss, *Disquisitiones arithmeticae* (1801), arts 294–98; *Werke*, I (1863) 349; *ibid* (German trans, Maser), pp 335–43 We here give essentially Dedekind's proof in Dirichlet's *Zahlentheorie* (2d ed, 1873; 3d ed, 1879; 4th ed, 1894), §§ 156 57 In *Norsk Matematisk Tidsskrift* X (1928), 50–54, T Skolem gave Dedekind's proof without employing index, but with a supplementary computation; an analogous proof had been given by Lagrange, *Mém Acad. Sc Berlin* XXIII (1769, année 1767), pp 385–406, *Œuvres*, II 384–99

I. Let (3) have integral solutions not all zero. After removal of common factors, we get a solution x, y, z whose g.c.d. is 1. Then if x and y have a common prime factor p, p^2 divides cz^2, but not c, whence p divides z, whereas p is not a common factor of x, y, z. In this way we see that x, y, z are relatively prime in pairs.

Then a and z are relatively prime. For, if they had a common prime factor p, by^2 would be divisible by p, whereas a is prime to b, and z to y. Hence $zw \equiv 1 \pmod{a}$ has a solution w. Multiplication of (3) by bw^2 yields $-bc \equiv (byw)^2 \pmod{a}$. The further cases (4) follow by symmetry.

II. Assume (1), (2), and (4) We shall prove that (3) is solvable. In case the positive integers

$$(5) \qquad |bc| \ , \quad |ca| \ , \quad |ab|$$

are all distinct, the *index* of (3) is defined to be that one of the three which lies between the remaining two But if two or three of the numbers (5) are equal, the index is defined as the common value of the two or three equal ones.

When the index is 1, at least one of the numbers (5) is 1, say $|ab|=1$. Then the numbers (5) are $|c|$, $|c|$, 1, whence $|c|=1$ by the definition of index. Since a, b, c are not all of like sign, we may take $a=1$, $b=-1$. Then (3) has the solution $x=1$, $y=1$, $z=0$. This proves the theorem for equations of index 1.

To proceed by induction, we assume that Theorem 91 holds for all such equations (3) whose index is $<J$, and prove it for index J. Hence let (3) have the index $J \geqq 2$. By the symmetry, we may assume that

$$(6) \qquad |a| \leqq |b| \leqq |c| \ .$$

Then $|ab| \leqq |ac| \leqq |bc|$, whence $J=|ac|$. Since b and c are relatively prime, $|b|=|c|$ would imply $|b|=|c|=1$,

and $|a|=1$ by (6), whence $J=1$, contrary to hypothesis. Hence

(7) $$|a| \leqq |b| < |c|\ , \quad |ab| < |ac| = J \leqq |bc|\ .$$

By (4) there exists a solution r of $ar^2 \equiv -b \pmod{c}$ such that $|r| \leqq \frac{1}{2}|c|$. We have

(8) $$ar^2 + b = cQ\ ,$$

(9) $$|Q| \leqq \frac{|a|r^2 + |b|}{|c|} \leqq \frac{1}{4}|ac| + \left|\frac{b}{c}\right| < \frac{1}{4}J + 1 < J\ .$$

The case $Q=0$ may be excluded. Since b is prime to a and has no square factor, $b=-ar^2$ implies $|r|=1$, $b=-a=\pm 1$, whence (3) has the solution $x=y=1$, $z=0$.

We shall reduce (3) to a similar equation of smaller index. Let A be the g.c.d. of the three terms of (8), whence A is the g.c.d. of any two of the three terms. Since A divides b, it is prime to a and c. Hence A divides r^2 and Q. But the divisor A of b has no square factor >1. Hence A divides r. We may write

(10) $$r = A\alpha, \quad b = A\beta, \quad Q = Aq = AC\gamma^2\ ,$$

where γ^2 is the largest square dividing q. Thus (8) gives

(11) $$aA\alpha^2 + \beta = cC\gamma^2$$

whose three terms are relatively prime in pairs. Write $B = a\beta$. We shall prove that

(12) $$AX^2 + BY^2 + CZ^2 = 0$$

has properties (1) and (2), while

(13) $-BC$, $-CA$, $-AB$ are quadratic residues of A, B, C, respectively

Evidently no one of A, B, C is zero. Since a and b are relatively prime and neither has a square factor >1.

$AB=ab$ implies that neither A nor B has a square factor >1, and that A and B are relatively prime. Since γ^2 is the largest square dividing $q=C\gamma^2$, C has no square factor >1. Since the terms of (11) are relatively prime in pairs, C is prime to $aA\beta=AB$.

Next, A, B, C are not all of the same sign. This is true if $ab=AB$ is negative. Hence let ab be positive. By (1), ca and bc are negative. Then

$$c(ar^2+b)=c^2Q=c^2AC\gamma^2$$

shows that AC is negative. This completes the proof that (12) has properties (1) and (2).

By (11), whose terms are relatively prime in pairs, we see that βcC, $acAC$, and $-aA\beta=-AB$ are quadratic residues of aA, β, and C, respectively. It remains to prove the first two parts of (13). By (4), $-bc=-\beta Ac$ and $-ca$ are quadratic residues of a and $b=A\beta$, respectively. Since βcC and $-ca$ are quadratic residues of A, the same is true of their product $-BCc^2$ and hence of $-BC$. Since $-ca$ and $acAC$ are quadratic residues of β, $-AC\equiv u^2 \pmod{\beta}$ has a solution u. Since βcC and $-\beta Ac$ are quadratic residues of a, $-AC\equiv v^2 \pmod{a}$ has a solution v. Since a and β are relatively prime by (11), there is a solution w of $w\equiv u \pmod{\beta}$, $w\equiv v \pmod{a}$. Hence $AC+w^2$ is divisible by β and a and hence by $\beta a=B$. This completes the proof of (13)

By (7), (9), and (10),

$$|AB|=|ab|<J\ , \quad |CA|\leq|CA|\gamma^2=|Q|<J\ .$$

Hence the index I of (12) is $<J$. By hypothesis, (12) has integral solutions X, Y, Z not all zero. Take

$$x=AaX-\beta Y\ , \quad y=X+aaY\ , \quad z=C\gamma Z\ .$$

Then by (10), (11), and $B=a\beta$, we get

$$ax^2+by^2+cz^2=cC\gamma^2(AX^2+BY^2+CZ^2)=0\ .$$

If $x=y=0$, elimination of X gives $(\beta+A\alpha a^2)Y=0$. The first factor is not zero by (11). Then $Y=0$, $X=0$, whence $Z=0$, contrary to what precedes. This proves Theorem 91 by induction.

Repetitions of our reduction of the index leads to an equation of index 1 having an evident solution. Hence our theory furnishes a method of solving (3).

COROLLARY. *Under assumptions* (1), (2), *and* (4), *equation* (3) *has a proper solution, i.e., with* x, y, z *relatively prime in pairs.*

EXERCISES XXXII

In Exs 1-3, C is positive and without square factor.

1. $x^2+y^2-Cz^2=0$ has integral solutions, not all zero, if and only if -1 is a quadratic residue of C, and hence if C is a sum of two relatively prime squares.

2. $x^2+2y^2-Cz^2=0$ with C odd is solvable if and only if -2 is a quadratic residue of C, and hence if C is represented properly by X^2+2Y^2 with X odd

3. $x^2+3y^2-Cz^2=0$ with C prime to 3 is solvable if and only if C and -3 are quadratic residues of each other, and hence if C is odd and represented properly by X^2+3Y^2.

4. $x^2-13y^2+23z^2=0$ is solvable

5. $x^2+41y^2-113z^2=0$ is solvable.

6 In (3) let a, b, c have no common factor >1 and no square factors. Let r denote the g c.d of b and c, s that of c and a, t that of a and b. Show that r, s, t are relatively prime in pairs. Then $a=stA$, $b=rtB$, $c=rsC$. Show that x/r, y/s, z/t are integers X, Y, Z. Deleting the factor rst from (3), we get

$$rAX^2+sBY^2+tCZ^2=0 .$$

Show that this equation has properties (1) and (2).

75. Problem. Given a proper solution u, v, w of an equation (3) having properties (1), to find all integral solutions.

The three terms of

$$(14) \qquad au^2+bv^2+cw^2=0$$

are relatively prime in pairs. For, if a prime p divides au and bv and hence also cw, either p divides a and hence neither b nor c, whence p divides v and w, contrary to assumption; or else p divides u and not v or w, whence p divides b and c, contrary to (1). Not all terms of (14) are odd. In view of the symmetry we may take au even. Then the g.c.d. of $2au$, bv, and cw is 1. Hence a linear combination of them is 1. Therefore

(15) $$auj+bvk+cwl=1, \quad j \text{ even},$$

has integral solutions. One of k and l is even and the other is odd. Write

(16) $$h=aj^2+bk^2+cl^2,$$

(17) $$U=2j-hu, \quad V=2k-hv, \quad W=2l-hw.$$

Since b and c are odd, h is odd. Also,

(18) $$aU^2+bV^2+cW^2=0,$$

(19) $$auU+bvV+cwW=2,$$

(20) $$u\equiv U, \quad v\equiv V, \quad w\equiv W \pmod 2.$$

Hence

(21) $$2u_1=vW-wV, \quad 2v_1=wU-uW, \quad 2w_1=uV-vU$$

determine integers u_1, v_1, w_1. From the identity

$$(bv^2+cw^2)(bV^2+cW^2)=(bvV+cwW)^2+bc(vW-wV)^2$$

and (14), (18), (19), and (21), we get

$$-au^2(-aU^2)=(2-auU)^2+4u_1^2bc,$$

which proves the first of the symmetrical results

(22) $$auU=1+bcu_1^2, \quad bvV=1+cav_1^2, \quad cwW=1+abw_1^2.$$

Adding these and applying (19), we get

(23) $$bcu_1^2+cav_1^2+abw_1^2=-1.$$

From the identity

$$(auU+bvV+cwW)(vW+wV)-a(wU-uW)(uV-vU)$$
$$\equiv(au^2+bv^2+cw^2)VW+(aU^2+bV^2+cW^2)vw\ ,$$

and (14), (18)–(21), we get the first of

$$(24)\qquad vW+wV=2av_1w_1\ ,\quad wU+uW=2bw_1u_1\ ,\quad uV+vU=2cu_1v_1\ .$$

If x, y, z are any integers, then

$$(25)\qquad t=aUx+bVy+cWz\ ,\quad t'=aux+bvy+cwz\ ,\quad \tau=u_1x+v_1y+w_1z$$

are integers which, by (20), satisfy

$$(26)\qquad t\equiv t' \pmod 2\ .$$

Conversely, if t, t', τ are any integers satisfying (26), the following values obtained from (22), (24), and (25):

$$(27)\qquad \begin{cases} 2x=ut+Ut'-2bcu_1\tau\ , \\ 2y=vt+Vt'-2cav_1\tau\ , \\ 2z=wt+Wt'-2abw_1\tau\ . \end{cases}$$

are even by (20) and (26), whence x, y, z are integers. Multiply equations (27) by ax, by, cz, respectively, add, and apply (25). We get

$$(28)\qquad ax^2+by^2+cz^2=tt'-abc\tau^2$$

Hence if x, y, z satisfy (3), the values of t, t', τ, computed from (25), satisfy (26) and

$$(29)\qquad tt'=abc\tau^2\ .$$

Conversely, if integers t, t', τ satisfy (26) and (29), the values of x, y, z computed by (27) are integers which satisfy (3).

To find all solutions of (29), let δ be the g.c.d. of t, t', τ, and let δL be the g.c.d. of δabc and t. Write $t=\delta Lr$, $abc=LK$. Then r is prime to K. Write $\tau=\delta\epsilon$. By (29), $rt'=K\delta\epsilon^2$. Hence $t'/\delta=Kq$, where q is an integer such that $rq=\epsilon^2$. Any common prime factor of q and r divides t/δ, t'/δ, $\epsilon=\tau/\delta$, whose g.c.d. is 1. Since q and r are relatively prime integers whose product is a square, each is a square: $q=n^2$, $r=m^2$, where the signs of n and m may be chosen so that $nm=+\epsilon$. Hence every solution of (29) is given by

$$(30) \qquad t=\delta Lm^2\,, \quad t'=\delta Kn^2\,, \quad \tau=\delta mn\,, \quad abc=KL\,,$$

such that the g.c.d. of Lm^2, Kn^2, and mn is 1. This requires

$$(31) \qquad n \text{ is prime to } m \text{ and } L,\ m \text{ is prime to } K\,.$$

By (31), the g.c.d. of Lm^2 and mn is m, and that of Kn^2 and mn is n, whence the g.c.d. of all three is 1.

Finally, (26) holds if and only if

$$(32) \qquad \delta \text{ even; or } \delta,\ m,\ n \text{ all odd, } K\equiv L \pmod 2\,.$$

For, if δ is odd, (26) holds only when Lm^2 and Kn^2 are both even or both odd. Then (31) shows that neither m nor n is even.

THEOREM 92. *If a, b, c are relatively prime in pairs and no one is zero, and if u, v, w is a proper solution of* (3), *we may assume that au is even and determine solutions j, k, l of* (15). *Express abc as a product KL of two integers in all ways. Let m, n, δ be any integers subject to the restrictions in* (31) *and* (32). *Employ the abbreviations* (16), (17), (21), *and* (30). *Then* (27) *yield integers which satisfy* (3), *and all integral solutions of* (3) *are so obtained.*

We may restrict L to positive values. If L is negative, we change the signs of L, K, δ, n, and see that (30) remain unaltered.

76. The case $a+b+c=0$. If z^2, x^2, y^2 are in arithmetical progression, then

$$(33) \qquad -2x^2+y^2+z^2=0\,.$$

Diophantus, *Arithmetica*, III, 9, noted the solution 41, 49, 31. In II, 20, and IV, 45, he obtained numerical solutions of

$$z^2-y^2:x^2-z^2=a:b$$

when a/b is $\frac{1}{3}$ or 3. This proportion is equivalent to (3) with $c=-a-b$. We may evidently assume that a is even and prime to b. We employ the proper solution $u=v=w=1$. Since $aj+bk=1$ has a solution with j even, we make take $l=0$ in (15). By (21), $u_1=-k$, $v_1=j$, $w_1=k-j$. Here $t-ht'$ is an even integer $2Q$, and (27) become

$$(34)\qquad x=Q+jt'+bck\tau\ ,\qquad y=Q+kt'-caj\tau\ ,\qquad z=Q-ab(k-j)\tau\ .$$

EXERCISES XXXIII

1. Solve (33). We may take $j=0$, $k=1$. Then

$$2x=t-t'+2\tau,\ 2y=t+t',\ 2z=t-t'+4\tau\ .$$

The last case in (32) is excluded, whence $\delta=2\rho$. If $L=1$, then $K=-2$, and m is odd and prime to n. Hence*

$$(35)\qquad x=\rho(m^2+2mn+2n^2),\qquad y=\rho(m^2-2n^2),\qquad z=\rho(m^2+4mn+2n^2)$$

In the remaining case $L=2$, $K=-1$, we interchange m and n and see that t, t' become $-t'$, $-t$ of the former case, whence the new solutions are obtained from the former by merely changing the sign of y.

2. In (33), $y\equiv z \pmod 2$. Hence $X=\frac{1}{2}(z-y)$, $Y=\frac{1}{2}(y+z)$, $Z=x$ are integers satisfying $X^2+Y^2=Z^2$. One of X and Y, say X, is even. Multiply the values in Ex. X, 1, by ρ. Replacing m by $m+n$, we get (35).

3. An automedian triangle is one whose medians are proportional to its sides x, y, z. If $y>x>z$, show that $y^2+z^2=2x^2$.

* In the thirteenth century, Jordanus Nemorarius noted the case $\rho=1$ of (35). Vieta (*Zetetica*, V, 2, 1591) took $x=z+n$, $y=m-z$, and obtained (35) with $\rho=1/(2m+4n)$

4. Solve $Ax^2+y^2-z^2=0$, when A has no square factor. We may take $u=j=l=0$, $v=w=k=1$. Then $h=V=1$, $U=v_1=w_1=0$, $W=u_1=-1$, $x=-\tau$, $2y=t+t'$, $2z=t-t'$. Write $\alpha=-L$, $\beta=K$. If δ is even, $\delta=-2\rho$, we get (5) of § 27. The second case in (32) is excluded if A is even. Hence let δ, m, n, K, L be all odd. Writing ρ for $-\delta$, we get (6) of § 27.

5. Solve $x^2+y^2-(\alpha^2+\beta^2)z^2=0$, when α is even and prime to β. We may take $u=\alpha$, $v=\beta$, $w=1$, $l=0$, j even, $\alpha j+\beta k=1$. Then $u_1=-k$, $v_1=j$, $w_1=\alpha k-\beta j$. Write $2Q$ for the even integer $t-ht'$. Then

$$x=\alpha Q+jt'-(\alpha^2+\beta^2)k\tau,\quad y=\beta Q+kt'+(\alpha^2+\beta^2)j\tau,$$
$$z=Q-(\alpha k-\beta j)\tau\ .$$

The values (30) are to be inserted.

Take $\alpha=2$, $\beta=1$, $j=0$, $k=1$. Then

$$x=t-t'-5\tau,\qquad y=\tfrac{1}{2}(t+t'),\qquad z=\tfrac{1}{2}(t-t')-2\tau\ .$$

If $L=5$, then $K=-1$. Replacing n by v and m by w, we see that y, x, z become the products of $\frac{1}{2}\delta$ by the respective numbers (19) in § 31 with the first changed in sign. When $L=1$, $K=-5$, we interchange m and n and find, as in Ex. 1, the former solution with y merely changed in sign. If we replace u by v and v by $-u$, we see that r and s of (18) in § 31 are merely changed in sign Why do all these facts give a new proof of Theorem 44?

77. Proper solutions of (3). By the Corollary before Ex. XXXII, there exist proper solutions if we include the assumption (2) that no coefficient has a square factor. We now discard that assumption and prove

THEOREM 93. *Let t and t' satisfy* (26) *and* (29), *and have no common odd divisor* >1. *Also, in case both t and t' are even, let*

$$t+t'\equiv 2\ (mod\ 4)\ . \tag{36}$$

Let u, v, w be a proper solution of (3) *having properties* (1). *Then x, y, z in* (27) *give a proper solution of* (3).

Let a prime p divide ax, by, and cz. By (25), p divides t and t', whence $p=2$. Then (20) and (25) imply $t+t'\equiv 0 \pmod 4$, which is contrary to (36). Hence the g.c.d. of ax, by, cz is 1. But if a prime divides x and y, it divides cz by (3). In this way we see that x, y, z are relatively prime in pairs.

LEMMA. *If* (3) *has properties* (1) *and is properly solvable, and if* $-bc$ *is a quadratic residue of* ap^2, *where* p *is a prime not dividing* bc, *then* (3) *has a proper solution such that* x *is divisible by* p.

We may assume that (3) has the proper solution u, v, w, where u is not divisible by p.

I. p odd. By hypothesis, $-bc\equiv \alpha^2 \pmod p$ holds for α prime to p. Hence $bcu_1+\alpha$ and $bcu_1-\alpha$ are not both divisible by p. The sign of α may be chosen so that the former is not divisible by p. Hence

$$(37) \qquad u\omega \equiv bcu_1+\alpha \pmod p$$

has a solution w prime to p. Write $2abc=p^nQ$, where $n\geqq 0$ and Q is prime to p. There exists a solution k of $\omega = w+kp\equiv 1 \pmod Q$. Thus (37) has a solution ω prime to both p and Q and hence to $2abc$. Choose

$$t=e\omega^2 , \qquad t'=eabc , \qquad \tau=e\omega ,$$

where $e=1$ or $e=2$, according as abc is odd or even. The resulting solution x, y, z of (3) is proper and has x divisible by p. For, if abc is odd, whence $e=1$, then $t\equiv t'\equiv 1 \pmod 2$. If abc is even, whence $e=2$, then $t\equiv 2$, $t'\equiv 0 \pmod 4$. Since ω is prime to abc, t and t' have no common odd divisor. Also, $tt'=abc\tau^2$. Theorem 93 shows that x, y, z give a proper solution of (3). By (27) and (22_1),

$$2x=e(u\omega^2+Uabc-2bcu_1\omega) ,$$

$$2ux=e[(u\omega-bcu_1)^2+bc]\equiv e(\alpha^2+bc)\equiv 0 \pmod p .$$

Hence x is divisible by p.

II. $p=2$. First, let a be even, but not divisible by 8. Since $-bc$ is a quadratic residue of $4a$, it is congruent to an odd square and hence to 1 modulo 8. Since bv and cw are prime to au, they are odd. Hence $b\equiv -b^2c\equiv -c$ (mod 8). Then $au^2\equiv 0$ by (14), and u is even, whereas u is not divisible by p.

Second, let $a\equiv 0$ (mod 8). As before, $-bc\equiv 1$ (mod 8). Take $\tau=1$. We may choose t and t' without a common odd factor >1 so that $t\equiv 2$, $t'\equiv 0$ (mod 4), $tt'=abc$. By Theorem 93, x, y, z give a proper solution of (3). By (22_1), u_1 is odd. Since also u is odd, (27) gives

$$2x\equiv 2+0-2\equiv 0 \pmod 4 , \quad x\equiv 0 \pmod 2 .$$

Third, let a be odd. Then $-bc\equiv 1$ (mod 4). Take $\tau=1$ and choose relatively prime integers t and t' whose product is abc. Then tt' is odd, whence $t\equiv t'$ (mod 2). By Theorem 93, x, y, z give a proper solution of (3). Since u and h are odd, $U=2j-hu$ is odd. By (22_1), u_1 is even and $auU\equiv 1$ (mod 4). Hence

$$ut\cdot Ut'=auU\cdot bc\equiv -1 , \quad ut\equiv -Ut' \pmod 4 .$$

By (27), $2x$ is divisible by 4.

THEOREM 94. *If* $A=aP^2$, $B=bQ^2$, $C=cR^2$ *are relatively prime in pairs, if* (13) *hold, and if* (3) *is properly solvable, then* (12) *is properly solvable.*

The mere fact that (12) is solvable follows by multiplying (3) by $P^2Q^2R^2$, whence

$$(38)\qquad A(QRx)^2+B(PRy)^2+C(PQz)^2=0 .$$

Since $-BC$ is a quadratic residue of A, $-bc$ is a quadratic residue of aP^2. Let P be a product of primes p, p_1, p_2, . . . , not necessarily distinct. Thus no one of p, p_1, . . . divides bc. Write a' for ap^2. The lemma applies and shows that $x=\xi p$ and that

$$(39)\qquad a'\xi^2+by^2+cz^2=0$$

has the proper solution ξ, y, z. Since $-bc$ is a quadratic residue of $a'p_1^2=a''$, the lemma states that (39) has a proper solution in which $\xi=\xi_1p_1$. In other words, $a''\xi_1^2+by^2+cz^2=0$ has a proper solution and hence one with ξ_1 divisible by p_2. Since the successive first coefficients are ap^2, $ap^2p_1^2$, $ap^2p_1^2p_2^2$, . . . , we ultimately reach $aP^2=A$, and conclude that

$$(40) \qquad AX^2+by^2+cz^2=0$$

is properly solvable. Since $-CA$ is a quadratic residue of B, $-cA$ is a quadratic residue of bQ^2. Let Q be a product of primes q, q_1, ... No one of them divides cA. The lemma states that (40) has a proper solution with $y=\eta q$. As before we obtain successive second coefficients bq^2, $bq^2q_1^2$, . . . , $bQ^2=B$. Finally, we may replace c by $cR^2=C$. Hence the lemma implies Theorem 94.

THEOREM 95. *If A, B, C are relatively prime in pairs, are not all of the same sign, and no one is zero, then $AX^2+BY^2+CZ^2=0$ is properly solvable if and only if $-BC$ is a quadratic residue of A, etc., cyclically as in* (13).

Note that this fundamental theorem is free of assumptions about square factors in A, B, or C.

Let (13) hold and let P^2, Q^2, and R^2 denote the largest squares dividing A, B, C, respectively. Then a, b, c in Theorem 94 have no square factors >1. Evidently (13) imply (4). By Theorem 91 and its corollary, (3) is properly solvable. Hence (12) is properly solvable by Theorem 94.

Conversely, let (12) be properly solvable and A, B, C be relatively prime in pairs. Then AX, BY, CZ are relatively prime in pairs by the first result in § 75. Hence there exist solutions ξ, η, ζ, of

$$Z\xi\equiv BY \pmod{A}\,, \qquad X\eta\equiv CZ \pmod{B}\,,$$
$$Y\zeta\equiv AX \pmod{C}\,.$$

Then (12) gives $B(BY^2+CZ^2)\equiv 0$, $\xi^2\equiv -BC \pmod{A}$. Similarly, $\eta^2\equiv -CA \pmod{B}$, $\zeta^2\equiv -AB \pmod{C}$.

EXERCISES XXXIV

1. Reduce the solution of $F\equiv AX^2+BY^2+CZ^2=0$ to a like equation whose coefficients have no square factors and are relatively prime in pairs. We may assume that the g.c.d. of A, B, C is 1. Write $A=aP^2$, $B=bQ^2$, $C=cR^2$, where a, b, c have no square factors. By (38), the solution of $F=0$ reduces to that of $f\equiv ax^2+by^2+cz^2=0$. Apply Ex. XXXII, 6.

2. Give another proof of Ex. 1. Let $A=p\alpha$, $B=p\beta$, where p is a prime. Then $Z=pz$ and $F/p=\alpha X^2+\beta Y^2+Cpz^2$. The product of its coefficients is ABC/p, which is numerically smaller than the product ABC for F. Repeat the process as long as any two coefficients have a common factor. We reach an F whose coefficients are relatively prime in pairs. Now apply (38).

78. Supplement to Theorem 95. In the proof of a chief result on genera in chapter ix, we shall need the following

THEOREM 96. *Assume properties* (1) *and* (4), *whence there exist integers* A, B, C *such that*

$$(41)\qquad A^2\equiv -bc \pmod{a}\,,\qquad B^2\equiv -ca \pmod{b}\,,\qquad C^2\equiv -ab \pmod{c}\,.$$

Then there exists a proper solution x, y, z *of* (3) *satisfying*

$$(42)\qquad Az\equiv by \pmod{a}\,,\quad Bx\equiv cz \pmod{b}\,,\quad Cy\equiv ax \pmod{c}\,.$$

By the Chinese remainder theorem there exist solutions of

$$(43)\qquad \begin{cases} X\equiv c \pmod{b}\,,\ Y\equiv a \pmod{c}\,,\ Z\equiv b \pmod{a}\,,\\ X\equiv C \pmod{c}\,,\ Y\equiv A \pmod{a}\,,\ Z\equiv B \pmod{b}\,.\end{cases}$$

Then (41) gives

$$(44)\qquad aX^2+bY^2+cZ^2\equiv 0 \pmod{abc}\,,$$

since the left member is divisible by a, b, and c. By Theorem 95, (3) has a proper solution u, v, w. Hence (14)–(29) hold. Write

$$(45)\quad T\equiv aUX+bVY+cWZ,\ T'\equiv auX+bvY+cwZ \pmod{2abc}.$$

By (20),

$$(46)\qquad T\equiv T' \pmod{2}.$$

By (22) and (24),

$$(47)\quad 2X\equiv uT+UT' \pmod{2bc},\ 2Y\equiv vT+VT' \pmod{2ca},\ 2Z\equiv wT+WT' \pmod{2ab}$$

Multiply these by aX, bY, and cZ, respectively, add, and apply (44) and (45). We get $0\equiv 2TT' \pmod{2abc}$, whence

$$(48)\qquad TT'\equiv 0 \pmod{abc}.$$

To show that T, T', and abc have no common odd prime factor p, let p divide them and c, for example. By (47), p divides Y. By (43), p divides $a\equiv Y \pmod{c}$. But a is prime to c.

By (43), conditions (42) are equivalent to

$$(49)\qquad Yz\equiv Zy \pmod{a},\qquad Zx\equiv Xz \pmod{b},\qquad Xy\equiv Yx \pmod{c}$$

From the values (25) and (45) of t, t', T, T',

$$\begin{vmatrix} T' & T \\ t' & t \end{vmatrix} \equiv ab(uV-vU)(Xy-Yx)-ac(wU-uW)(Xz-Zx) + bc(vW-wV)(Yz-Zy) \pmod{2abc}.$$

By (21) this becomes

$$(50)\quad T't-Tt'\equiv 2abw_1(Xy-Yx)-2acv_1(Xz-Zx) + 2bcu_1(Yz-Zy) \pmod{2abc}.$$

Evidently (49) and (50) imply

(51) $$T't \equiv Tt' \pmod{2abc} .$$

Conversely, (50) and (51) imply (49). For, by (22), u_1, v_1, w_1 are relatively prime to a, b, c, respectively. Since $0 \equiv 2bcu_1(Yz-Zy) \pmod{2a}$, $Yz-Zy$ is divisible by a.

Hence conditions (42) are equivalent to the single condition (51). To prove Theorem 96 it suffices to show that we can choose t, t', τ to satisfy (51) and the conditions in Theorem 93.

I. abc odd. Let d denote the g.c.d. of T and $abc=dd'$. By (48), d' divides $T' \cdot T/d$ and hence also T'. We saw that T, T', and abc have no common (odd) divisor. Since they are divisible by any common factor of d and d', the latter are relatively prime. The g.c.d. 1 of T, T', abc is also the g.c.d. of d and $T'=d' \cdot T'/d'$. Hence 1 is the g.c.d. of d and T'/d'. Hence d' is the g.c.d. of $dd'=abc$ and T'. We take $t=d$, $t'=d'$, $\tau=1$. Since t and t' are odd, (26) holds. Evidently (29) holds. Also, t and t' are odd and relatively prime. By Theorem 93, x, y, z give a proper solution of (3) By (26) and (46), $T't$ and Tt' are congruent modulo 2 and are divisible by dd'; hence (51) holds.

II. abc even. Then T and T' are even by (46) and (48). Suppose that $T' \equiv T \pmod 4$. By symmetry, let c be even. Then (47) implies $2Y \equiv (v+V)T \pmod 4$. By (20), $v+V$ is even. Hence Y is even. Since $a \equiv Y \pmod c$ by (43), a is even. But a is prime to c. This contradiction shows that $T+T' \equiv 2 \pmod 4$. By symmetry, we may take $T \equiv 0$, $T' \equiv 2 \pmod 4$. Define d and d' as in (I)

If d' is odd, take $t=2d$, $t'=2d'$, $\tau=2$. Then $t \equiv 0$, $t' \equiv 2 \pmod 4$. Evidently $tt'=abc\tau^2$. Also, $T't$ and Tt' are divisible by $2dd'$, whence (51) holds. Finally, d and d' and hence t and t' have no common odd divisor. By Theorem 93, x, y, z give a proper solution of (3).

If d' is even, take $t=d$, $t'=d'$, $\tau=1$. Since T/d is prime to d' and hence is odd, $T\equiv 0$ implies $d\equiv 0 \pmod 4$. Since d' divides T', $T'\equiv 2$ implies $d'\equiv 2 \pmod 4$. Hence $t\equiv 0$, $t'\equiv 2 \pmod 4$. By (I), t and t' have no common odd divisor. Hence Theorem 93 applies. Since T/d and T'/d' are odd, their difference is even. Multiplying it by $dd'=abc$, we get (51).

EXERCISES XXXV

1. Let x, y, z be a proper solution satisfying (42), and u, v, w a given such solution. By (27)

$$0\equiv Bx-cz\equiv \tfrac{1}{2}Gt+\tfrac{1}{2}Jt' \pmod b\ , \tag{52}$$

where $G=Bu-cw$, $J=BU-cW$. By (14), (22), (42), $G\equiv 0$, $uwJ\equiv -2u \pmod b$. In (14), uw is prime to b. If b is odd, J is prime to b and t' is divisible by b. Prove the last also if b is even. Hence t' is always divisible by abc.

2. Let x_1, y_1, z_1 be another proper solution satisfying (42) Let it arise from t_1, t'_1, τ_1. By (26), $tt_1'-t't_1$ is divisible by $2abc$. Conversely, this fact implies that the corresponding proper solutions satisfy the same congruences (42).

3. The common factor δ in (30) divides the expressions (27), whence $\delta=1$ or 2. Since t' is divisible by $abc=KL$, δn^2 is divisible by L. Hence L divides δ. If abc is odd, then $L=1$, $K=abc$.

CHAPTER IX

COMPOSITION AND GENERA OF BINARY QUADRATIC FORMS

79. Introduction. We shall prove that the product of two related quadratic forms q and Q can be expressed as a third quadratic form, which is said to be derived from them by *composition*. For the case $q=Q$, see (39) of § 53. We shall then develop the theory of genera, a topic already found useful in §§ 52–55.

Lemma 1. *Let $m, t_1, \ldots, t_n$ have the greatest common divisor 1. If m divides every $t_r q_s - q_r t_s$ $(r, s=1, \ldots, n)$, there is one and only one solution B of*

(1) $$t_1 B \equiv q_1, \ldots, t_n B \equiv q_n \pmod{m}.$$

Since 1 is a linear combination of $m, t_1, \ldots, t_n$ (§ 1), there exist integers h_s such that $\Sigma t_s h_s \equiv 1 \pmod{m}$. Denote $\Sigma q_s h_s$ by β. Then

$$t_r\beta = \Sigma t_r q_s h_s \equiv \Sigma q_r t_s h_s = q_r \Sigma t_s h_s \equiv q_r \pmod{m},$$

whence β is a solution B of (1). Multiplying (1) by $h_1, \ldots, h_n$, respectively, and adding, we get $B\equiv\beta \pmod{m}$.

Lemma 2. *If $b^2\equiv d \pmod{4a}$, $\beta^2\equiv d \pmod{4\alpha}$, and if*

(2) $$a,\ \alpha,\ \tfrac{1}{2}(b+\beta) \text{ have no common factor } >1,$$

there exists a solution B of

(3) $$B\equiv b \pmod{2a},\quad B\equiv\beta \pmod{2\alpha},\quad B^2\equiv d \pmod{4a\alpha},$$

and B is uniquely determined modulo $2a\alpha$. Also, a, α, B have no common factor >1.

Congruences (3) imply

(4) $$\alpha B\equiv \alpha b,\quad aB\equiv a\beta,\quad \tfrac{1}{2}(b+\beta)B\equiv\tfrac{1}{2}(d+b\beta) \pmod{2a\alpha}.$$

We obtain the third from

$$0\equiv(B-b)(B-\beta)=B^2+b\beta-(b+\beta)B,\quad B^2\equiv d \pmod{4a\alpha}\ .$$

Conversely, (4) imply (3). Lemma 1 with $m=2a\alpha$ may be applied to (4) since the three coefficients of B have 1 as their g.c.d., and since

$$\alpha\cdot a\beta-\alpha b\cdot a\ ,\quad \alpha\cdot\tfrac{1}{2}(d+b\beta)-\tfrac{1}{2}(b+\beta)\alpha b=\tfrac{1}{2}\alpha(d-b^2)\ ,$$
$$a\cdot\tfrac{1}{2}(d+b\beta)-\tfrac{1}{2}(b+\beta)a\beta=\tfrac{1}{2}a(d-\beta^2)$$

are all divisible by $2a\alpha=m$. Hence (3) have a solution B which is unique modulo $2a\alpha$.

If D is a common divisor of a, α, B, (3) give

$$B\equiv b\equiv\beta\ ,\quad \tfrac{1}{2}(b+\beta)\equiv B \pmod{D}\ .$$

Since D divides the three numbers (2), $D=1$.

LEMMA 3. *If* $f=ax^2+Bxy+\alpha Cy^2$, $\phi=\alpha\xi^2+B\xi\eta+aC\eta^2$, *then*

$$(5)\qquad f\phi=F\ ,\quad F=a\alpha X^2+BXY+CY^2\ ,$$

$$(6)\qquad X=x\xi-Cy\eta\ ,\qquad Y=ax\eta+\alpha y\xi+By\eta\ .$$

If $\delta=\sqrt{d}$, $d=B^2-4a\alpha C$, direct multiplication gives

$$(7)\quad [2ax+(B+\delta)y][2\alpha\xi+(B+\delta)\eta]=4a\alpha X+2(B+\delta)Y$$

Replace δ by $-\delta$ and multiply together. We get

$$4af\cdot 4\alpha\phi=16a\alpha F\ .$$

80. Composition. Two integral forms $r=[a,\ b,\ c]$ and $\rho=[\alpha,\ \beta,\ \gamma]$ are called *united* if they have the same discriminant d and if (2) holds. Then all of the assumptions made in Lemma 2 hold, whence there exists a solution B of congruences (3), and the g.c.d. of a, α, and B is 1.

By (3_3), $B^2-d=4a\alpha C$, where C is an integer. Hence the discriminant of $F=[a\alpha,\ B,\ C]$ is d.

By (3_1), $B=b+2ak$. In $r=ax^2+bxy+cy^2$ we replace x

by $x+ky$ and obtain the form $f=[a, B, \alpha C]$, which is therefore called *parallel* to r. Conversely, if we replace x by $x-ky$ in f, we get r.

By (3_2), $B=\beta+2\alpha l$. In $\rho=\alpha\xi^2+\beta\xi\eta+\gamma\eta^2$ we replace ξ by $\xi+l\eta$ and obtain the parallel form $\phi=[\alpha, B, aC]$.

In Lemma 3 we replace x by $x-ky$ and ξ by $\xi-l\eta$ and obtain $r\rho=F$, where the present variables in F are derived from (6) by these replacements. Hence F is said to be derived from r and ρ by *composition.*

For the special composition (5), f and ϕ are united forms since they have the same discriminant d and since the g.c.d. of a, α, $B=\frac{1}{2}(B+B)$ is 1.

If we replace B by a new solution $B+2a\alpha t$ of (3), we replace F by a parallel form F_1 which is derived from F by replacing X by $X+tY$. Evidently F_1 is derived from r and ρ by composition.

Parallel forms r and f are equivalent and hence belong to the same class. We shall reach the goal of composition of classes when we prove

THEOREM 97. *For all choices of two united forms from two classes k and κ, the forms derived from them by composition belong to a unique class, denoted by either $k\kappa$ or κk, and said to be derived from k and κ by composition.*

Stated otherwise, if the united forms r and ρ are equivalent to the united forms $[m, n, l]$ and $[\mu, \nu, \lambda]$, respectively, then the forms F and $E=[m\mu, N, L]$ derived from the pairs by composition are equivalent.

In the proof we may replace r by f, ρ by ϕ, and similarly the second pair by $e=[m, N, \mu L]$ and $\epsilon=[\mu, N, mL]$. Given that $f\backsim e$ and $\phi\backsim\epsilon$, we are to prove that $F\backsim E$. We apply the criterion for equivalence in § 56. Since $f\backsim e$ and $\phi\backsim\epsilon$, there exist integers x, y, ξ, η satisfying

$$(8) \qquad m=ax^2+Bxy+\alpha Cy^2, \qquad \mu=\alpha\xi^2+B\xi\eta+aC\eta^2\ ,$$

(9) $2ax+(B+N)y\equiv 0\ ,\quad (B-N)x+2\alpha Cy\equiv 0 \pmod{2m}\ ,$

(10) $2\alpha\xi+(B+N)\eta\equiv 0\ ,\quad (B-N)\xi+2aC\eta\equiv 0 \pmod{2\mu}\ .$

To prove that $F\backsim E$ by the same criterion it suffices to show that there exist integers X and Y satisfying

(11) $$m\mu=a\alpha X^2+BXY+CY^2\ ,$$

(12) $$2a\alpha X+(B+N)Y\equiv 0 \pmod{2m\mu}$$

(13) $$(B-N)X+2CY\equiv 0 \pmod{2m\mu}\ .$$

Evidently (11) follows from (5), (6), and (8). Let

(14) $$(t+s\delta)(\tau+\sigma\delta)=T+S\delta\ ,\qquad \delta=\sqrt{d}$$

whence $S=t\sigma+s\tau$, $T=t\tau+ds\sigma$. Then

$$(t+sz)(\tau+\sigma z)=T+Sz+s\sigma(z^2-d)\ ,$$

identically in z. Let d be the discriminant of our forms. Then $d=N^2-4m\mu L$. Taking $z=N$, we get

(15) $$(t+sN)(\tau+\sigma N)\equiv T+SN \pmod{4m\mu}\ .$$

Now (7) is a known case of (14) with

$$t=2ax+By,\ s=y,\ \tau=2\alpha\xi+B\eta,\qquad \sigma=\eta,$$
$$T=4a\alpha X+2BY,\qquad S=2Y$$

The factors on the left of (15) are multiples of $2m$ and 2μ, respectively, by (9) and (10). This proves (12).

The proof of (13) is longer. Multiply the first or second factor in (7) by $B-\delta$ and divide by $2a$ or 2α, respectively. We get

(16) $$[(B-\delta)x+2aCy][2\alpha\xi+(B+\delta)\eta]=2aR\ ,$$

(17) $$[2ax+(B+\delta)y][(B-\delta)\xi+2aC\eta]=2aR\ ,$$

where $R=(B-\delta)X+2CY$. Multiply (16) by $B+\delta$ and (17) by $B-\delta$, we get

$$C[2ax+(B+\delta)y][2\alpha\xi+(B+\delta)\eta]=(B+\delta)R\ ,$$
$$[(B-\delta)x+2aCy][(B-\delta)\xi+2aC\eta]=(B-\delta)R\ .$$

Replacing δ by N we obtain congruences modulo $4m\mu$ since (14) implies (15). In view of (9) and (10), each first factor becomes a multiple of $2m$ and each second factor becomes a multiple of 2μ. Also, R becomes the left member L of (13). Hence $(B \pm N)L$ are divisible by $4m\mu$. Similarly, by (16) and (17), $2\alpha L$ and $2aL$ are divisible by $4m\mu$. Hence $2m\mu$ divides the products of L by α, a, B, whose g.c.d. is 1, and therefore divides L. This proves (13).

81. What classes k and κ admit composition? The g.c.d. of the coefficients of a form is called its *divisor*. Equivalent forms have the same divisor, which is called the divisor of their class.

THEOREM 98. *If s is the divisor of $f=[a, B, \alpha C]$ and σ is that of $\phi=[\alpha, B, aC]$, and if f and ϕ are united, the form $F=[a\alpha, B, C]$ derived from them by composition has the divisor $s\sigma$, while s and σ are relatively prime.*

By definition of united, the g.c.d. of a, α, B is 1. The divisor s of a and B is prime to α (and hence to the divisor σ of α). Since s divides αC, it divides C. Similarly, the divisor σ of α and B is prime to a; it divides aC and hence C. Since the relatively prime numbers s and σ divide B and C, $s\sigma$ divides them and evidently also $a\alpha$.

If possible, let the quotients of $a\alpha$, B, C by $s\sigma$ have a common prime factor p. Then p divides a/s or α/σ. If p divides a/s, ps is a common divisor of a, B, αC, whereas s is their g.c.d. Similarly, p is not a divisor of α/σ. This contradiction shows that $s\sigma$ is the g.c.d. of $a\alpha$, B, C and hence that $s\sigma$ is the divisor of F.

THEOREM 99. *If the classes k and κ have the same discriminant d and have relatively prime divisors s and σ, we can select united forms $[a, b, c]$ and $[\alpha, \beta, \gamma]$ from k and κ, respectively, such that a/s and α/σ are prime to any assigned integer n.*

Select any form h of class k. By Theorem 66 the primitive form h/s represents properly an integer a/s which is

prime to σ and n. As in § 46, h is equivalent to a form $[a, b, c]$ with the first coefficient a. If a and σ have a common prime factor p, then s is not divisible by p, and a/s and σ would have the common factor p, contrary to what precedes. Hence a is prime to σ.

Similarly, we can choose $[\alpha, \beta, \gamma]$ from the class κ so that α/σ is prime to a and n. If a and α have a common prime factor q, the divisor q of a is prime to σ, and α/σ has the factor q in common with a. This contradiction shows that a and α are relatively prime. Hence $[a, b, c]$ and $[\alpha, \beta, \gamma]$ are united.

We may combine Theorems 98 and 99 into

THEOREM 100. *Two classes k and κ admit composition if and only if they have the same discriminant d and their divisors s and σ are relatively prime, and then $k\kappa$ has the divisor $s\sigma$ and discriminant d.*

82. Associative law for composition. Let s, σ, S be the divisors of classes k, κ, K. Let the class $k\kappa \cdot K$ exist. Then s is prime to σ, and S is prime to $s\sigma$. As in the proof of Theorem 99, we can choose $[a, b, c]$ in k so that a/s is prime to σS, whence a is prime to σS; then choose $[\alpha, \beta, \gamma]$ in κ so that α/σ is prime to aS, whence α is prime to aS; then choose $[A, B, C]$ in K so that A/S is prime to $a\alpha$. Suppose that A and $a\alpha$ have a common prime factor p. If S were not divisible by p, A/S and $a\alpha$ would have the factor p. Hence p divides S and therefore divides neither a nor α. This contradiction shows that A is prime to $a\alpha$. We saw that α is prime to a.

Since k, κ, K have the same discriminant d, b, β, B are all even or all odd. At most one of a, α, A is even. First let α and A be odd. Then $2a$, α, and A are relatively prime in pairs and there is a solution r of

$$r \equiv b \pmod{2a}, \quad r \equiv \beta \pmod{\alpha}, \quad r \equiv B \pmod{A}$$

Then $r \equiv b \equiv \beta \equiv B \pmod 2$, whence

$$r \equiv b \pmod{2a}, \quad r \equiv \beta \pmod{2\alpha}, \quad r \equiv B \pmod{2A}$$

In case a and A are odd, we use the moduli a, 2α, A and obtain the last result. If a and α are odd, we use moduli a, α, $2A$. We have

$$d = b^2 - 4ac \equiv b^2 \equiv r^2 \pmod{4a}, \quad d \equiv \beta^2 \equiv r^2 \pmod{4\alpha},$$
$$d \equiv B^2 \equiv r^2 \pmod{4A}$$

Hence $r^2 - d$ is divisible by $4a\alpha A$; let s denote the quotient. Then the classes k, κ, K, $k\kappa$, and κK contain the respective forms

$$[a, r, \alpha As], \quad [\alpha, r, aAs], \quad [A, r, a\alpha s], \quad [a\alpha, r, As],$$
$$[\alpha A, r, as],$$

all of discriminant d. Since $k\kappa \cdot K$ and $k \cdot \kappa K$ both contain $[a\alpha A, r, s]$, they are identical classes and may be denoted by $k\kappa K$.

THEOREM 101. *Composition of classes obeys the associative law.*

EXERCISES XXXVI

1. According as $d \equiv 0$ or $1 \pmod 4$, $[1, 0, -d/4]$ or $[1, 1, \frac{1}{4}(1-d)]$ is called the *principal form* P of discriminant d. Let $f = [a, b, c]$ be any form of the same discriminant d. In P we replace x by $x + ty$, where $t = \frac{1}{2}b$ or $\frac{1}{2}(b-1)$ in the respective cases, and get $[1, b, ac]$. The latter and f are united and give f by composition. The class containing P is called the *principal class* and denoted by 1. Hence $1 \cdot k = k \cdot 1 = k$ for every class k.

2. If $f = [a, b, c]$ is primitive, f and $[c, b, a]$ are united and give $[ac, b, 1]$ by composition. The latter is equivalent to $[1, -b, ac]$ and hence to P. Also, $[c, b, a] \backsim [a, -b, c]$, which is *opposite* to f. Hence if k and k' are opposite, primitive classes, $kk' = k'k = 1$ Thus k' is denoted by k^{-1} and called *inverse* to k.

3. Hence if k is a primitive class $k\kappa = kK$ implies $\kappa = K$.

4. If $d = -31$, the three positive, reduced forms $[1, 1, 8]$,

$f=[2, -1, 4]$, and $g=[2, 1, 4]$ belong to classes 1, k, $k^{-1}=k^3$. Hint: For f, a solution of (3) is $B=-1$. By composition of f with itself, we get $[4, -1, 2] \backsim g$.

5. If $d=-23$, the three positive, reduced forms [1, 1, 6], $f=[2, -1, 3]$, and $g=[2, 1, 3]$ belong to classes 1, k, $k^{-1}=k^2$. Hint: $f \backsim \phi=[2, 3, 4]$ whose $B=3$ satisfies (3). By composition of ϕ with itself, we get $[4, 3, 2] \backsim [2, -3, 4] \backsim g$.

6. If $d=-39$, the reduced, positive forms [1, 1, 10], [2, −1, 5], [3, 3, 4], [2, 1, 5] belong to classes 1, k, k^2, k^3.

7. If $d=-84$, the reduced, positive forms [1, 0, 21], $f=[3, 0, 7]$, $h=[2, 2, 11]$, $g=[5, 4, 5]$ belong to classes 1, k, κ, $k\kappa$, where $k^2=\kappa^2=1$. Hints: There is no composition of f with itself. Use f and [7, 0, 3], $B=0$. Next, $f \backsim [3, 6, 10]$, $h \backsim [2, 6, 15]$, whose composition gives $[6, 6, 5] \backsim [5, -6, 6] \backsim g$. To verify $\kappa^2=1$, the compound of $[2, -2, 11] \backsim h$ with $[11, -2, 2] \backsim h$ is $[22, -2, 1] \backsim [1, 2, 22] \backsim 1, 0, 21]$.

8. If $d=-96$, the reduced, positive forms [1, 0, 24], [3, 0, 8], [5, 2, 5], [4, 4, 7] belong to classes 1, k, κ, $k\kappa$, with $k^2=\kappa^2=1$.

9. If $d=-224$, the reduced, positive forms [1, 0, 56], [5, 4, 12], [8, 8, 9], [5, −4, 12], [4, 4, 15], [3, 2, 19], [7, 0, 8], [3, −2, 19] belong to classes 1, k, k^2, k^3, K, Kk, Kk^2, Kk^3, with $k^4=K^2=1$.

83. Number of genera. Consider primitive* forms with even middle coefficient: $q=ax^2+2bxy+cy^2$. Our former notation for q was $[a, 2b, c]$. We now employ Gauss's notation (a, b, c). Its determinant is $D=b^2-ac$ and discriminant is $4D$. In case D is negative, we assume that q is a positive form. We defined the characters of q in § 53.

LEMMA 4. *Any two primitive classes admit composition. If t and τ are the values of a character C for the classes k and κ, then $t\tau$ is the value of C for the class $k\kappa$.*

By Theorem 99 we can select from k and κ two united forms whose first coefficients a and α are both prime to $2D$. The form derived from them by composition is in

* Often called properly primitive. The improperly primitive forms q have a and c even, while $\frac{1}{2}q$ is primitive.

class $k\kappa$ and has $a\alpha$ as first coefficient. From the definition of characters it follows at once that

$$C(a) \cdot C(\alpha) = C(a\alpha) , \tag{18}$$

which proves Lemma 4.

Since the principal class contains $x^2 - Dy^2$, which represents 1, all its characters have the value $+1$. The genus which contains the principal class is called the *principal genus*. Hence for any form in it, the value of every character is $+1$.

LEMMA 5. *If classes k and κ belong to the same genus and if k' and κ' belong to one genus, then kk' and $\kappa\kappa'$ belong to one genus.*

For, a character C then has the same value v for k and κ, and the same value v' for k' and κ'. Hence by Lemma 4, C has the value vv' for both kk' and $\kappa\kappa'$.

If P is any class in the principal genus, (18) shows that any character C has the same value for K as for PK, whence classes K and PK belong to the same genus.

In particular, if P and P' are classes in the principal genus, PP' is in the principal genus. Since opposite forms evidently represent the same integers, any character has the same value for each form. Hence by Ex. XXXVI, 2, the class inverse to P is in the principal genus. In view of these two properties and the associative law of composition, the p classes in the principal genus are said to form a *group* π.

We can arrange all the h primitive classes into g sets

$$\pi, \pi H_2, \pi H_3, \ldots, \pi H_g$$

such that no two of these sets overlap. To do this, choose as H_2 any class not in π; choose as H_3 any class in neither π nor the set πH_2; etc. If the sets πH_2 and πH_3 had a class

in common, so that $P'H_2 = PH_3$, then would $H_3 = P_1H_2$, where $P_1 = P^{-1}P'$ is in π, contrary to the definition of H_3.

We saw that all classes of a set πH_i (where $H_1 = 1$) belong to the same genus. Different sets belong to different genera. For, if a character C has the same value for $P'H_2$ and PH_3, C has the same value for H_2 and H_3, and hence the value $+1$ for $H_3H_2^{-1}$. If this is true for every C, then $H_3H_2^{-1}$ is a class P_1 of the principal genus, whence $H_3 = P_1H_2$, contrary to the definition of H_3. This proves

THEOREM 102. *If h is the number of all primitive classes of a given determinant and p is the number in the principal genus, then $h = pg$, where g is the number of genera. The number of classes in every genus is p.*

Lemma 4 implies that if each character has the same value for k as for κ, then all characters for $k\kappa$ are $+1$. In other words, if k and κ belong to the same genus, then $k\kappa$ is in the principal genus.

The class k^2 is said to be derived from k by *duplication*. Thus every class Q which arises by duplication belongs to the principal genus. Hence if there are q distinct classes Q, evidently $q \leqq p$.

Let Q arise by duplication from both k and κ. Write A for κk^{-1}, whence $\kappa = Ak$. Thus $k^2 = Q = \kappa^2 = A^2k^2$, $A^2 = 1$, or $A = A^{-1}$. Hence every form (a, b, c) of A is equivalent to its opposite form $(a, -b, c)$ and hence is imporperly equivalent to itself. Then (a, b, c) is equivalent to an ambiguous form (the double of whose middle literal coefficient is divisible by its first coefficient). This was proved in § 43 for positive forms and in § 72 for indefinite forms. Then A is called an *ambiguous class.*

The a ambiguous classes A evidently form a group $\mathfrak{A}$. As in the proof of Theorem 102, all h classes fall into t non-overlapping sets $\mathfrak{A}, \mathfrak{A}H_2, \ldots, \mathfrak{A}H_t$, such that H_2 is not in $\mathfrak{A}$, H_3 is in neither $\mathfrak{A}$ nor $\mathfrak{A}H_2$, etc. Evidently the

α classes in $\mathfrak{A}H$, have the same square H_1^2. We proved that the square of no further class is H_1^2. Hence $t=q$. This proves

THEOREM 103. *If exactly q classes Q arise by duplication, and if α is the number of ambiguous classes, the number of all primitive classes is $h=q\alpha$. Each Q arises by duplication from exactly α classes.*

Since $q\leqq p$, Theorems 102 and 103 give $g\leqq\alpha$.

84. Number α of ambiguous classes. We employ only properly primitive, ambiguous forms $f=(a, b, c)$ of determinant D. Since $2b\equiv0$ or $a \pmod{2a}$, f is equivalent to $(a, 0, c)$ or $(2b, b, c)$ in new letters. We postpone the case $D=-1$.

In $(a, 0, c)$, $ac=-D$, and a and c are relatively prime. If n denotes the number of distinct prime factors of D, $|D|$ has exactly 2^n resolutions into two positive, relatively prime factors, since the highest power of any prime dividing D must be taken into one of the two factors. The two factors are distinct, since otherwise they would both be 1, whence $|D|=1$. The first factor and its negative are permissible values of a. Hence there are exactly 2^n pairs of forms $(a, 0, c)$ and $(c, 0, a)$, and those of any pair are equivalent.

In $(2b, b, c)$, $b^2-2bc=D$, whence b is a positive or negative divisor of D. Write $D=-bb'$, whence $c=\frac{1}{2}(b+b')$. Since the form is primitive, c is odd and prime to b. Hence b and b' have no common odd divisor and $b+b'\equiv2 \pmod 4$.

If b is odd, then $b'\equiv b$, $D\equiv3 \pmod 4$. Conversely, $D\equiv3 \pmod 4$ implies that b, b', c are all odd. Thus b can be chosen as any divisor of D such that b and b' are relatively prime. Hence if b is odd, *there are 2^{n+1} primitive forms $(2b, b, \frac{1}{2}[b+b'])$, half of which have b positive.* Also, $|b|\neq|b'|$.

If b is even, one of b and b' is $\equiv0$ and the other is $\equiv2$

(mod 4). Hence $D\equiv 0 \pmod 8$ and $\frac{1}{2}b$ and $\frac{1}{2}b'$ are relatively prime. Conversely, if $D\equiv 0 \pmod 8$, b and b' must be even, and $\frac{1}{2}b$ can be chosen as any divisor of $\frac{1}{4}D$ such that $\frac{1}{2}b$ and $\frac{1}{2}b'$ are relatively prime. Since $\frac{1}{4}D$ is even, it has the same number n of distinct prime factors as D. Hence the italicized statement holds also if b is even. Also, $|\frac{1}{2}b|$ and $|\frac{1}{2}b'|$ are distinct, since one is even and the other is odd.

Whether b is odd or even, there are exactly 2^n pairs

$$(2b,\ b,\ \tfrac{1}{2}[b+b']) \ , \quad (2b',\ b',\ \tfrac{1}{2}[b+b'])$$

of primitive forms. The transformation $\begin{pmatrix}-1 & -1\\ 2 & 1\end{pmatrix}$ of determinant 1 replaces the first by the second.

We retain only that form of each pair whose first coefficient is the smaller numerically. Hence we have 2^n forms or no form of each of the types

$$(a,\ 0,\ c)\ , \qquad (2b,\ b,\ \tfrac{1}{2}[b+b'])\ , \tag{19}$$

in which a^2 and b^2 are $<|D|$.

Let m be the number of distinct *odd* prime factors of D. Then $n=m$ or $m+1$, according as D is odd or even. If $D\equiv 1 \pmod 4$, only the first forms (19) occur and their number is 2^m. If $D\equiv 3 \pmod 4$ or $D\equiv 0 \pmod 8$, both occur and their number is 2^{m+1} or 2^{m+2}, respectively. If $D\equiv 2, 4, 6 \pmod 8$, only the first occur and their number is 2^{m+1}. In each case, the exponent of 2 is the number* k of characters defined in § 53.

The system of values (each 1 or -1) of the various characters of a given form is called a *total character* of the form. Hence there are $T=2^k$ total characters of primitive forms of determinant D.

Hence the number of forms (19) is T.

*Omitting $\delta\epsilon$ if both δ and ϵ are characters

I. Let D be negative. We retain only the forms (19) with positive outer coefficients. We shall prove that no two of the resulting positive forms are equivalent. Each $(a, 0, c)$ is semi-reduced. The same is true of the second form q in (19) if $c = \frac{1}{2}(b+b') \geqq 2b$. But if $c < 2b$, q has the semi-reduced right neighboring form $(c, c-b, c)$. Since no middle coefficient is negative, no two of the resulting semi-reduced forms

$$(a, 0, c)\ , \quad (2b, b, c)\ , \quad (c, c-b, c)$$

are opposite or identical. By Theorem 52, no two are equivalent. Hence the number a of positive, primitive, ambiguous classes of negative determinant D is $\frac{1}{2}T$. This holds also for the excluded case $D=-1$, since $(1, 0, 1)$ is then the only reduced, positive form, while $T=2$.

II. Let $D>0$. If (A, B, C) is any one of the forms (19), there is evidently a unique integer β satisfying

$$(20) \quad \beta \equiv B \pmod{A}\ , \qquad 0<\delta-\beta<|A| \qquad (\delta=\sqrt{D})\ .$$

Determine an integer γ so that $\beta^2 - A\gamma = D$. Then (A, B, C) is parallel and hence equivalent to (A, β, γ). The conditions that the latter be reduced are

$$(21) \qquad \beta<\delta\ , \quad \delta-\beta<|A|<\delta+\beta\ .$$

Hence it remains only to prove that

$$(22) \qquad |A|<\delta+\beta\ .$$

If $|A|<\delta$, (20) gives $\delta-\beta<\delta$, whence $\beta>0$ and (22) follows.

If $|A|>\delta$, the first form (19) is excluded, whence $A=2B$ and $B^2<\delta^2$. Then $\beta=|B|$ satisfies (20) since $0<\delta-|B|<\delta<|A|$, and (22) holds.

We now prove that every reduced, primitive, ambigu-

ous form (r, s, t) is identical with one of these (A, β, γ). As in (21),

$$0<s<\delta\ , \qquad \delta-s<|r|<\delta+s\ .$$

First, let s be divisible by r, $s=rq$. Then $|r|\cdot|q|<\delta$, whence $|r|<\delta$, and the form $(r, 0, r')\sim(r, s, t)$ is one of the forms (A, B, C). To get its corresponding form (A, β, γ), we determine β by (20), viz., $\beta\equiv 0 \pmod r$, $0<\delta-\beta<|r|$. These hold if $\beta=s$, whence (A, β, γ) is (r, s, t).

Second, let $2s\equiv r \pmod{2r}$. Then $2s=rq$, where q is odd. Thus $|r|\cdot|q|<2\delta$, $|r|<2\delta$, and the form $(r, \frac{1}{2}r, t')\sim(r, s, t)$ is one of the (A, B, C). As before, its corresponding (A, β, γ) is (r, s, t).

Hence the number of reduced, primitive, ambiguous forms is T. By Theorem 90 every ambiguous class contains exactly two reduced, ambiguous forms. This completes the proof of

THEOREM 104. *The number a of properly primitive, ambiguous classes (which are positive if $D<0$) of determinant D is half the number T of total characters.*

We saw that $g\leqq a$. Hence $g\leqq\frac{1}{2}T$.

EXERCISES XXXVII

(For δ and ϵ see § 53)

1. If $D=-21$, the characters are $(n|3)$, $(n|7)$, and δ, whence $T=8$. By Ex. XXXVI, 7, all four positive classes are ambiguous, and $a=4=\frac{1}{2}T$.

2. If $D=-24$, the characters are $(n|3)$, δ, ϵ. All four positive classes are ambiguous. See the example in § 53 and Ex. XXXVI, 8.

3. If $D=-56$, the characters are $(n|7)$, δ, ϵ. The four positive ambiguous classes are 1, k^2, K, k^2K in Ex. XXXVI, 9.

4. If $D=\pm p\equiv 1 \pmod 4$, where p is a prime >2, the single character is $(n|p)$. Then $g\leqq 1$, $g=1$, and all (positive) primitive forms (a, b, c) belong to the principal genus. Hence $(a|p)=1$ if a is not divisible by p (§ 53 n.). Since $a=1$, the only ambiguous class is the principal class.

5. Check Ex. 4 for $D=-23$ and $D=-31$ by means of Exs. XXXVI, 4, 5. Hints: $k=(k^{-1})^2$, and every form which arises by duplication is in the principal genus.

6. Gauss gave the following proof of the reciprocity law for positive primes p, q. First, let one of them, say p, be $\equiv 1 \pmod 4$. If $(q|p)=1$, then $(-q|p)=1$ and we can choose the sign so that $\pm q \equiv 1 \pmod 4$, $b^2-pc \equiv \pm q$, whence (p, b, c) has determinant $\pm q$, and $(p|q)=1$ by Ex. 4. Prove the converse by use of (q, B, C) of determinant p. Second, let $p\equiv q\equiv 3 \pmod 4$. For forms of determinant pq, the only characters are $(n|p)$ and $(n|q)$. The latter are 1, 1 for $(1, 0, -pq)$, but are $-1, -1$ for $(-1, 0, pq)$ since a form represents its first coefficient. But $g \leqq \frac{1}{2}T=2$. Hence there are exactly two genera. Thus any primitive form has one of the total characters 1, 1 and $-1, -1$. Since $(p, 0, -q)$ represents p and $-q$, we have either

$$(p|q)=(-q|p)=+1 \text{ or } (p|q)=(-q|p)=-1 \; .$$

In the first case, $(q|p)=-1$; in the second case, $(q|p)=+1$. Hence if $p\equiv q\equiv 3 \pmod 4$, $(p|q)(q|p)=-1$ in both cases.

7. Show that $g \leqq \frac{1}{2}T$ by the generalized reciprocity Theorem 39. We may write $D=\pm 2^a PS^2$, where $a=0$ or 1, and P is a product of distinct, odd primes. Use the abbreviations $t=\frac{1}{2}(\pm P-1)$, $k=(-1)^t$, $l=(-1)^a$, $f=\frac{1}{8}(n^2-1)$, $m=\frac{1}{2}(n-1)$, where n is any positive integer prime to $2D$. Then

$$(2|n)^a=(-1)^{fa}=l^f \; , \quad (\pm P|n)=(-1)^{tm}(n|P) \; ,$$

$$(D|n)=(2|n)^a(\pm P|n)=k^m l^f (n|P) \; .$$

If n is any positive integer, prime to $2D$, which is represented properly by a form of determinant D, there is a root of $N^2\equiv D \pmod n$ by (32) of § 46, whence $(D|n)=1$. Thus

$$\pi=k^m l^f (n|P)=+1 \; .$$

Examine the various cases for D in Theorem 67 and verify that π is always either a character or a product of characters, except when $k=l=P=1$, and then $D=S^2$, an excluded case. Hence the characters satisfy the relation $\pi=1$ and are dependent. If there be a single character C, then C is always $+1$.

8. Check Ex. 7 by noting that $\epsilon(n|3)=1$ for every form in the table in § 53. In Ex. 1, $\delta(n|3)(n|7)=1$. In Ex. 2, $\epsilon(n|3)=1$. In Ex. 3, $\epsilon(n|7)=1$.

85. Gauss's celebrated theorem on duplication. The proof by Gauss employed quadratic forms in three variables. It was proved in 1864 by Kronecker by the analytic methods which had been employed by Dirichlet in his proof of Theorem 106. We shall follow the proof by Dedekind, which is closely related to the proof by Arndt in *Jour. für Math.*, Volume LVI (1859).

THEOREM 105. *Every primitive class of the principal genus arises by duplication, the class being positive if* $D<0$.

As representative of a given class of the principal genus, choose a form (A, B, C) of determinant D with A prime to $2D$. Since all its characters are $+1$, A is a quadratic residue of every odd prime factor of D and also of 4 or 8 in case D is divisible by 4 or 8. For, in the respective cases in § 53, $\delta=+1$, $A\equiv 1 \pmod 4$; $\delta=\epsilon=1$, $A\equiv 1 \pmod 4$, $A^2\equiv 1 \pmod{16}$, whence $A\equiv 1 \pmod 8$. The last implies that A is a quadratic residue of every power of 2 by Theorem 17. Hence A is a quadratic residue of D.

Without loss of generality we may assume that A is a quadratic residue of $4D$, viz., $A\equiv 1 \pmod 4$ or $A\equiv 1 \pmod 8$, according as D is odd or even. This is already true if $D\equiv 3 \pmod 4$ or $D\equiv 0 \pmod 8$. Suppose that A does not satisfy the respective congruence in the remaining cases. Then $A\equiv 3 \pmod 4$, $A\equiv 7$, 3, or 5 (mod 8), according as $D\equiv 1 \pmod 4$, $D\equiv 2$, 6, or 4 (mod 8), respectively, since $\epsilon=1$, $\delta\epsilon=1$, or $\delta=1$ in the last three cases. The transformation

$$\begin{pmatrix} a & -1 \\ 1 & 0 \end{pmatrix}$$

replaces (A, B, C) by an equivalent form whose first coefficient is $A'=Aa^2+2Ba+C$. Then $AA'=(Aa+B)^2-D$.

Choose α so that $A\alpha+B$ is even in the first case and odd in the remaining three cases, and such that $A\alpha+B$ is prime to D. Then A' has the desired properties and is prime to $2D$.

By the definition of D, $4D\equiv(2B)^2 \pmod{A}$. Hence $4D$ and A are quadratic residues of each other. Also A and D are not both negative. By Theorem 96,

$$(23) \qquad Ax^2+4Dy^2-z^2=0$$

holds for integers relatively prime in pairs satisfying $2Bz\equiv 4Dy \pmod{A}$. Hence $z\equiv 2By \pmod{A}$. We may write $z=Aw+2By$. In (23) we replace z by this value and D by B^2-AC, and divide the result by A. We get

$$Aw^2+2Bw(2y)+C(2y)^2=x^2 .$$

In (23), Ax, $4Dy$, and z are relatively prime in pairs. Since z is therefore odd, w is odd. If a prime divides w and y, it would divide z. Hence w is prime to $2y$, and x^2 is represented properly by (A, B, C). Hence the latter is equivalent to a form (x^2, u, v) whose first coefficient x^2 is prime to $4D$. This form arises by duplication from (x, u, xv) since any common factor of x and u would divide $u^2-x^2v=D$.

COROLLARY. If (A, B, C) is a primitive form of the principal genus of determinant D (positive if $D<0$), then

$$Ax^2+2Bxy+Cy^2=z^2$$

is solvable in integers with z prime to $2D$.

86. Theorem 106. *The number g of (positive) primitive genera is half the number T of total characters.*

By Theorems 102–5, $h=pg=q\alpha$, $\alpha=\frac{1}{2}T$, $q=p$. Hence $g=\alpha=\frac{1}{2}T$.

CHAPTER X

DIOPHANTINE EQUATIONS WITH ONLY A FINITE NUMBER OF INTEGRAL SOLUTIONS

87. Summary. A polynomial $f(z)$ with rational coefficients is called *reducible* if it is a product of two polynomials each of degree $\geqq 1$ with rational coefficients. When it is not such a product, it is called *irreducible.* For example, x^2-4 is reducible and x^2-2 is irreducible.

By Ex. XXX, 5, Pell's equation $x^2-Dy^2=1$ has infinitely many integral solutions if D is positive and not a square. This is in contrast to the remarkable theorem due to Thue:*

THEOREM 107. *Let* $f(z)=a_nz^n+\ldots+a_0$ *be an irreducible polynomial of degree* $n\geqq 3$ *with integral coefficients. Consider the corresponding homogeneous polynomial*

$$(1)\qquad H(x, y)=a_nx^n+a_{n-1}x^{n-1}y+\cdots+a_1xy^{n-1}+a_0y^n\,.$$

If c *is an integer,* $H(x, y)=c$ *has either no solution or only a finite number of solutions in integers.*

We shall obtain a like theorem for $H=G(x, y)$ and for $ay^2+by+c=dx^n$. Although the proofs are long, they are strictly elementary and presuppose only calculus.

The proofs rest on the following theorem† of Thue on the rational approximation to a root of an algebraic equation:

* *Jour. für Math.*, CXXXV (1909), 284–305 A gap in his proof was filled by Maillet, *Nouv. Ann. Math.*, XVI (1916), 338–45

† We shall follow the proof by Siegel, *Videnskapsselskapets Skrifter*, Vol 1 (1921), as presented by Landau, *Zahlentheorie*, III (1927), 37–65

THEOREM 108. *Let θ be a root of an irreducible equation of degree $n \geqq 3$ with integral coefficients. Let $A > 0$. Then*

$$\left| \theta - \frac{x}{y} \right| < \frac{A}{y^n} \tag{2}$$

holds for only a finite number of pairs of integers x, $y > 0$.

88. Properties of an irreducible polynomial.

THEOREM 109. *Let $f(z)$ and $g(z)$ be polynomials with rational coefficients and let $f(z)$ be irreducible. If one root θ of $f(z)=0$ satisfies $g(z)=0$, then $f(z)$ is a divisor of $g(z)$.*

Let $d(z)$ be the g.c.d. of $f(z)$ and $g(z)$. The method explained in elementary algebra for finding $d(z)$ is similar to that in § 1 and shows that $d(z)$ has rational coefficients Here $d(z)$ has the factor $z-\theta$ and is not a constant. By the irreducibility of $f(z)$, the quotient of $f(z)$ by $d(z)$ is a constant $c \neq 0$. But $g = dQ$. Hence $g = f \cdot Q/c$.

When $f(z)$ is irreducible, $f(z)=0$ is called irreducible.

COROLLARY 1. *An irreducible equation has no root in common with an equation of lower degree having rational coefficients.*

COROLLARY 2. *The roots of an irreducible equation are all distinct.*

For, if $f(z)=0$ has a multiple root θ, $f'(\theta)=0$.

89. Theorem 108 implies Theorem 107. Note that

$$\frac{H(x, y)}{y^n} = f\left(\frac{x}{y}\right) \qquad \text{if } y \neq 0\ . \tag{3}$$

I. Let $c=0$. Then $H=0$ has only the solution $x=y=0$ in integers. For, evidently $y=0$ implies $x=0$. If there were a solution in integers x', y' with $y' \neq 0$, then $f(z')=0$ for $z'=x'/y'$, and $f(z)$ would have the factor $z-z'$, contrary to its irreducibility.

II. Let $c \neq 0$. To $y=0$ corresponds at most two integers x with $a_n x^n = c$. We first show that $H=c$ has only a

finite number of integral solutions with $y>0$. Let $\theta_1, \ldots, \theta_n$ be the roots of $f(z)=0$. Consider integers x, y for which

$$H(x, y)=a_n(x-\theta_1 y) \ldots (x-\theta_n y)=c\,, \qquad y>0\,.$$

Then

$$|a_n| \cdot \prod_{k=1}^{n} |x-\theta_k y| = |c|\,. \tag{4}$$

Hence there is at least one k for which

$$|x-\theta_k y| \leqq C_1\,, \qquad C_1^n = \left|\frac{c}{a_n}\right|.$$

The roots of the irreducible equation $f(z)=0$ are all distinct by Corollary 2. Hence for each $j\neq k$, $|\theta_k-\theta_j|$ exceeds a constant $C_2>0$, and

$$|x-\theta_j y| = |(\theta_k-\theta_j)y+(x-\theta_k y)| > C_2 y - C_1 > \tfrac{1}{2}C_2 y\,,$$

when $y>2C_1/C_2$. Then

$$\prod_{j\neq k} |x-\theta_j y| > (\tfrac{1}{2}C_2 y)^{n-1}\,.$$

Hence (4) gives

$$|x-\theta_k y| < \frac{C_3}{y^{n-1}}\,, \qquad C_3=\frac{|c|}{|a_n|\,(\frac{1}{2}C_2)^{n-1}}\,,$$

or $|\theta_k - x/y| < C_3/y^n$. Taking $A=C_3$ and $\theta=\theta_k$, we conclude from Theorem 108 that y belongs to a finite set of integers >0. To each y corresponds at most n integers x for which $H(x, y)=c$.

Second, consider integral solutions with $y<0$. Since $f(z)$ is irreducible, the same is true of $(-1)^n f(-z)$, to which corresponds $H(x, -y)$. By the first case, $H(x, -y)=c$ has only a finite number of integral solutions with $y>0$. Hence $H(x, Y)=c$ has only a finite number of integral solutions with $Y<0$.

90. Linear dependence. Polynomials $P_1(x), \ldots, P_m(x)$ with rational coefficients will be called *linearly independent* if an identity $c_1P_1 + \ldots + c_mP_m \equiv 0$ holds for rational $c_1, \ldots, c_m$ only when the latter are all zero. But if such an identity holds when the rational c's are not all zero, then $P_1, \ldots, P_m$ are called *linearly dependent*. For example, x^2 and $2x$ are independent, while x^2 and $2x^2$ are dependent. These definitions are used also when $m=1$; P is called independent or dependent, according as P is not or is identically zero.

THEOREM 110 (Wronski). *Let $P_{jm}(x)$ denote the jth derivative of the polynomial $P_m(x)$. If the determinant*

$$W = |P_{jk}(x)| \qquad (j=0, 1, \ldots, m-1; k=1, \ldots, m)$$

is identically zero, $P_1, \ldots, P_m$ are linearly dependent.

When $m=1$, $W=P_1$ and the theorem holds. To proceed by induction on m, let the theorem hold when m is replaced by $m-1$. In case $P_1, \ldots, P_{m-1}$ are dependent, evidently $P_1, \ldots, P_m$ are dependent. We need therefore prove the theorem only when $P_1, \ldots, P_{m-1}$ are linearly independent. Then our assumption for the induction shows that

$$D = |P_{jk}(x)| \qquad (j=0, 1, \ldots, m-2; k=1, \ldots, m-1)$$

is not identically zero. Hence $D \neq 0$ for all real x's between certain limits a and b. We can therefore solve the equations

$$(5) \qquad \sum_{k=1}^{m-1} P_{jk}(x)y_k = P_{jm}(x) \qquad (j=0, 1, \ldots, m-2)$$

uniquely for the y_k. Insert these values of P_{jm} into the mth column of W. For $k=1, \ldots, m-1$, multiply the kth column by $-y_k$ and add the products to the mth column.

In the new mth column, all elements are zero, except the bottom element, which is the left member L of

(6) $$P_{m-1,m}-\sum_{k=1}^{m-1}P_{m-1,k}y_k=0\,.$$

Then $0=W=DL$, whence $L=0$.

By the differentiation of (5), we get

$$\sum_{k=1}^{m-1}P_{j+1,k}y_k+\sum_{k=1}^{m-1}P_{jk}y_k'=P_{j+1,m}\,.$$

If $j<m-2$, we employ (5) with j replaced by $j+1$. But if $j=m-2$, we use (6). In either case,

$$\sum_{k=1}^{m-1}P_{jk}y_k'=0 \qquad (j=0,\,1,\,\ldots,\,m-2)\,.$$

But $D\neq 0$ if $a<x<b$. Then each $y_k'=0$, whence y_k is a constant C_k. Since the solutions y_k of (5) are rational functions of x with rational coefficients, each C_k is a rational number. The case $j=0$ of (5) now gives

$$\Sigma P_k(x)C_k-P_m(x)=0$$

for $a<x<b$ and hence for all x. Thus $P_1,\ldots,P_m$ are dependent.

91. Four lemmas. In these lemmas, needed for the proof of Theorem 108, θ is a root of an irreducible equation

(7) $$\psi(x)=x^n+\ldots=0$$

of degree $n\geqq 3$ with integral coefficients; $0<\delta<1$; g and s are given positive integers, $s<n$; $c_0,\ldots,c_7$ are positive integers depending on θ and δ, but not on g or s. For a real x, $[x]$ denotes the largest integer $\leqq x$. Finally,

(8) $$m=\left[\left(\frac{n+\delta}{s+1}-1\right)g\right]\,.$$

LEMMA 1. *There exists c_0 and a polynomial*

$$R(x, y) = \sum_{i=0}^{m+g} \sum_{j=0}^{s} b_{ij} x^i y^j , \tag{9}$$

whose coefficients are integers not all zero, such that

$$|b_{ij}| \leqq c_0^g \qquad (0 \leqq i \leqq m+g,\ 0 \leqq j \leqq s) . \tag{10}$$

Also, $R(x, \theta)$ is divisible by $(x-\theta)^g$. Hence if we write

$$R_l(x, y) = \frac{1}{l!} \frac{\partial^l R(x, y)}{\partial x^l} , \tag{11}$$

then

$$R_l(\theta, \theta) = 0 \qquad (l = 0, 1, \dots, g-1) . \tag{12}$$

Let $\theta_1, \dots, \theta_n$ be the roots of (7). Write

$$c_1 = 1 + [\text{Max. of } |\theta_1| , \dots , |\theta_n|] , \quad c_2 = 2(1+c_1), \quad c_3 = c_2^{2n} ,$$

$$c_4 = 1 + [(3c_3)^{n/\delta}] , \quad c_0 = 2c_1 , \quad a = c_4^g , \quad t = ac_3^g ,$$

$$N = (2a+1)^{(m+g+1)(s+1)} . \tag{13}$$

Then

$$c_4 > (3c_3)^{n/\delta} , \qquad a > 3^{n/\delta} c_3^{gn/\delta} , \qquad a^{n/\delta} > (3ac_3^g)^n = (3t)^n .$$

Since $m+1$ exceeds the quantity in brackets in (8),

$$m+g+1 > \frac{(n+\delta)g}{s+1} ,$$

$$N > a^{(n+\delta)g} > (3t)^{ng} . \tag{14}$$

Consider the N polynomials

$$P(x, y) = \sum_{i=0}^{m+g} \sum_{j=0}^{s} B_{ij} x^i y^j , \qquad |B_{ij}| \leqq a , \tag{15}$$

with integral coefficients each chosen from $2a+1$ values. Employ notation (11) with P in place of R; then

$$P_l(x, y)=\sum_{i=l}^{m+g}\sum_{j=0}^{s}\binom{i}{l}B_{ij}x^{i-l}y^j ,$$

$$\left|\binom{i}{l}B_{ij}\right|\leqq\binom{m+g}{l}a<(1+1)^{m+g}a=2^{m+g}a=b ,$$

where b is a new abbreviation. For $k=1, \ldots, n$, we have $|\theta_k|<c_1$ and

$$|P_l(\theta_k, \theta_k)|<b\sum_{i=l}^{m+g}\sum_{j=0}^{s}c_1^{i-l}c_1^j\leqq b(1+c_1)^{m+g}(1+c_1)^s$$
$$<2^{m+g+s}a(1+c_1)^{m+g+s}=ac_2^{m+g+s} .$$

By (8),

$$m<\left(\frac{n+1}{s+1}-1\right)g , \qquad m+g+s<\frac{n+1}{2}\cdot g+n<ng+ng .$$

Hence

$$(16) \qquad |P_l(\theta_k, \theta_k)|<ac_2^{2ng}=ac_3^g=t .$$

Of the roots of (7), let $\theta_1, \ldots, \theta_r$ be real and θ_k and θ_{k+c} be conjugate imaginary for $r<k\leqq r+c$. Thus there are r real and c pairs of complex roots, where either r or c may be zero.

Let α denote any one of the g numbers $P_l(\theta, \theta)$, where $0\leqq l\leqq g-1$. To α we make correspond n real numbers $\alpha_1, \ldots, \alpha_n$ defined by

$$\alpha_k=P_l(\theta_k, \theta_k) \qquad (k=1, \ldots, r) ,$$
$$\alpha_k+i\alpha_{c+k}=P_l(\theta_k, \theta_k) \qquad (k=r+1, \ldots, r+c)$$

If for such a complex number P we denote its real component by $\Re P$ and the coefficient of i by $\Im P$, we have

$$a_k = \Re P_l(\theta_k, \theta_k) \qquad (k = r+1, \ldots, r+c) ,$$
$$a_k = \Im P_l(\theta_{k-c}, \theta_{k-c}) \qquad (k = r+c+1, \ldots, r+2c) .$$

By (16), $|a_k| < t$ for $k = 1, \ldots, n$.

For each of the N polynomials (15) we therefore have gn numbers a_k which may be regarded as co-ordinates of a point within a "cube" of edge $2t$ in gn-dimensional space.* We divide this cube into $(3t)^{gn}$ congruent smaller cubes each with an edge $2t/(3t) = \frac{2}{3}$. By (14), we have more points than small cubes. Hence at least two of the points belong to a certain small cube. Let these two points arise from the polynomials P^* and $P^\dagger$ of type (15). Each of their coefficients is numerically $\leqq a$. Write

$$R(x, y) = P^*(x, y) - P^\dagger(x, y) .$$

This R is of the form (9). We have (10) since

$$|b_{ij}| \leqq a + a = 2c_4^g \leqq (2c_4)^g = c_0^g .$$

Let $0 \leqq l \leqq g-1$ and use the temporary abbreviations

$$\rho = R_l(\theta_k, \theta_k) , \quad A = P_l^*(\theta_k, \theta_k) , \quad B = P_l^\dagger(\theta_k , \theta_k) .$$

For $1 \leqq k \leqq r$, A and B are corresponding co-ordinates of two points in a cube of edge $\frac{2}{3}$, whence $|\rho| = |A - B| \leqq \frac{2}{3}$.

For $r+1 \leqq k \leqq r+c$, we have

$$|\Re\rho| = |\Re A - \Re B| \leqq \tfrac{2}{3} , \quad |\Im\rho| = |\Im A - \Im B| \leqq \tfrac{2}{3} ,$$

whence $|\rho| \leqq \frac{2}{3}\sqrt{2} < 1$. Since θ_k and θ_{k+c} are conjugate imaginary,

$$|R_l(\theta_{k+c}, \theta_{k+c})| = |\rho| < 1.$$

* This convenient geometrical language may be readily replaced by arithmetical statements concerning the gn numbers a_k. For a single number (or one dimension), the entire proof is similar to that in § 96.

Hence $|\rho|<1$ for $k=1, \ldots, n$. Thus the product

$$R_l(\theta_1, \theta_1) \ldots R_l(\theta_n, \theta_n)$$

is numerically <1. Being a symmetric function with integral coefficients of the roots of (7), it is an integer. Hence it is zero. Thus $\rho=0$ for a certain k. Since the polynomial $R_l(z, z)$ with rational coefficients vanishes for one root of an irreducible equation (7), it vanishes for all its roots (Theorem 109). Hence (12) holds

LEMMA 2. *If* $R(x, y)$ *has the properties in Lemma* 1 *and if* $x-\theta=u$, $y-\theta=v$, $|u|\leqq 1$, $|v|\leqq 1$, *then*

$$|R_l(x, y)| \leqq c^g\{|u|^{g-l}+|v|\} \quad (0\leqq l\leqq g-1) .$$

By (9) and (10),

$$R_l(x, y)=\sum_{k=0}^{m+g-l}\sum_{j=0}^{s} d_{kj}\, x^k y^j ,$$

(17) $$|d_{kj}|=\binom{k+l}{l}|b_{k+l,\,j}|\leqq\binom{m+g}{l}c^g<(1+1)^{m+g}c_0^g<c_6^g ,$$

if $c_6=2^{n+1}c_0$, since by (8)

$$m<\frac{n+1}{s+1}\,g\leqq\frac{n+1}{2}\,g<ng .$$

Evidently

(18) $$R_l(x, y)=\sum_{k,\,j} d_{kj}(u+\theta)^k(v+\theta)^j=\sum_{k,\,j} e_{kj}\, u^k v^j .$$

By Lemma 1, $R_l(x, \theta)$ is divisible by u^{g-l}. Hence

(19) $$R_l(x, y)=u^{g-l}\sum_{k=g-l}^{m+g-l} e_{k0}\,u^{k-g+l}+v\sum_{k=0}^{m+g-l}\sum_{j=1}^{s} e_{kj}\,u^k v^{j-1}$$

Comparing the coefficients of $u^p v^q$ in the two sums in (18), we get

$$e_{pq}=\sum_{k,j}\binom{k}{p}\binom{j}{q}d_{kj}\theta^{k-p}\theta^{j-q} .$$

Thus

$$|e_{pq}|\leqq\sum_{k,j}|d_{kj}|(|\theta|+1)^k(|\theta|+1)^j .$$

But $|\theta|<c_1$ and the number of summands is $\leqq(m+g+1)\cdot(s+1)$. Applying also (17), we see that

$$|e_{pq}|<(m+g+1)(s+1)c_6^g(c_1+1)^{m+g}(c_1+1)^s<c_7^g ,$$

by choice of a positive integer c_7 independent of g and s. Hence by (19), if $|u|\leqq 1$, $|v|\leqq 1$,

$$|R_l(x, y)\leqq|u|^{\sigma-l}c_7^g\,\Sigma\,1+|v|c_7^g\,\Sigma\Sigma\,1 .$$

Hence there is a positive integer c_8, independent of g and s, such that Lemma 2 holds.

LEMMA 3. *Let $R(x, y)$ have the properties in Lemma 1, so that we may write*

$$R(x, y)=\sum_{j=0}^{s}f_j(x)y^j$$

where each $f_j(x)$ is a polynomial with integral coefficients of degree $\leqq m+g$. Let $\sigma+1$, but not more, of the f, be linearly independent. Let the $f_{j_q}(x)$ for $q=0, \ldots, \sigma$ be linearly independent, whence by Theorem 110 the determinant

$$W(x)=|f_{j_q}^{(p)}(x)| \qquad (p=0, \ldots, \sigma;\, q=0, \ldots, \sigma)$$

involving the pth derivatives of the f, is not identically zero. Let $g>n$ and let a rational number h be given. There exists an integer γ, depending only on θ, s, δ, g, h, such that $0\leqq\gamma\leqq\delta g+n^2-n$, while, for the γth derivative of $W(x)$,

$$W^{(\gamma)}(h)\neq 0 .$$

Here $\sigma \leqq s < n < g$, and every $f_i(x)$ may be expressed as a linear function of the $f_{j_q}(x)$ with $q \leqq \sigma$ with rational coefficients. Then

$$R(x, y) = \sum_{q=0}^{\sigma} f_{j_q}(x) U_q(y) , \tag{20}$$

where the U's are polynomials with rational coefficients of degrees $\leqq s$. No $U_q(y)$ is identically zero, since the coefficient of y^{j_q} in it is 1. By (11) and (20),

$$p!\, R_p(x, y) = \sum_{q=0}^{\sigma} f_{j_q}^{(p)}(x) U_q(y) \qquad (0 \leqq p \leqq \sigma) . \tag{21}$$

By Lemma 1, $R_p(x, \theta)$ is divisible by $(x-\theta)^{g-p}$ and hence by $(x-\theta)^{g-\sigma}$. The same is therefore true of the sum in (21) for $y = \theta$. We multiply the latter by the cofactor of $f_{j_0}^{(p)}(x)$ in $W(x)$, sum for $p = 0, \ldots, \sigma$, and get $W(x) U_0(\theta)$. The degree of $U_0(y)$ is $\leqq s < n$; hence $U_0(y)$ vanishes for no root of the irreducible equation (7) of degree n (Corollary 1). Since $U_0(\theta) \neq 0$, $W(x)$ is divisible by $(x-\theta)^{g-\sigma}$. The exponent is positive. Since $W(x)$ vanishes for the root θ of the irreducible equation $f(x) = 0$ in (7), we have $W \equiv fQ$ by Theorem 109. If $g - \sigma > 1$, we see similarly that $Q \equiv fQ_1$, etc. Hence

$$W(x) = \{f(x)\}^{g-\sigma} D(x) , \tag{22}$$

where the polynomial $D(x)$ has rational coefficients not all zero. Let d be the degree of $D(x)$.

Each element of determinant W of order $\sigma + 1$ is either identically zero or is of degree $\leqq m + g$. Hence W is of degree $\leqq (\sigma+1)(m+g)$. Hence by (8) and (22),

$$d \leqq (\sigma+1)(m+g) - n(g-\sigma) \leqq (s+1)\, \frac{n+\delta}{s+1}\, g - ng + ns$$
$$= \delta g + ns \leqq \delta g + n(n-1) .$$

Since h is a rational number, $f(h)\neq 0$. By (22), if W is divisible by $(x-h)^{\gamma}$, but by no higher power, then $\gamma \leqq d$. This proves Lemma 3.

LEMMA 4. *Let K be prime to $E>0$, and k prime to $e>c_0^g$. Let $g\geqq 2n^2$, $\delta<\frac{1}{2}$. There exists an integer l depending on θ, s, δ, g, K, E, k, e, and exists a positive integer c depending on θ and δ such that $0\leqq l<\delta g+n^2$ and*

$$(23)\qquad c^g E^{m+g} e^g M>1, \qquad M=Max.\ of \left|\theta-\frac{K}{E}\right|^{g-l},\quad \left|\theta-\frac{k}{e}\right| .$$

We may assume that

$$(24)\qquad \left|\theta-\frac{K}{E}\right|\leqq 1\,, \qquad \left|\theta-\frac{k}{e}\right|\leqq 1\,.$$

For, if either were >1, (23) holds for $l=0$. Next, in (9),

$$R(x, y)=\sum_{i=0}^{m+g}\phi_i(y)x^i\,.$$

If every $\phi_i(k/e)=0$, select an i such that $\phi_i(y)$ is not identically zero. Evidently e divides the coefficient of the highest power of y in $\phi_i(y)$. By (10) that coefficient is numerically $\leqq c_0^g$. Hence $e\leqq c_0^g$, contrary to hypothesis. This shows that $R(x, k/e)$ is not identically zero. Hence in (20) there is a q for which $U_q(k/e)\neq 0$. Since we may permute the functions $f_{i_q}(x)$ in Lemma 3, we may take $U_0(k/e)\neq 0$ without loss of generality.

Multiply (21) with $y=k/e$ by the cofactor of $f_{j_0}^{(p)}(x)$ in the determinant $W(x)$, sum for $p=0, \ldots, \sigma$, and get

$$(25)\qquad W(x)U_0\left(\frac{k}{e}\right)=\sum_{p=0}^{\sigma}T_p(x)R_p\left(x, \frac{k}{e}\right),$$

where $T(x)$ is a polynomial with rational coefficients. By Lemma 3 with $h=K/E$, there exists an integer γ such that

$$0 \leqq \gamma \leqq \delta g + n^2 - n\ , \qquad W^{(\gamma)}\left(\frac{K}{E}\right) \neq 0\ .$$

Then by (25) there are rational numbers u_j for which

$$W^{(\gamma)}\left(\frac{K}{E}\right) U_0\left(\frac{k}{e}\right) = \sum_{j=0}^{\sigma+\gamma} u_j R_j\left(\frac{K}{E}\ ,\ \frac{k}{e}\right)\ .$$

Since the left member is not zero, the same is true of some summand on the right, say that given by $j=l$. Then

$$0 \leqq l \leqq \sigma + \gamma < n + \gamma \leqq \delta g + n^2\ ,$$
$$S \equiv R_l\left(\frac{K}{E}\ ,\ \frac{k}{e}\right) \neq 0\ .$$

By the hypothesis, we get $l < \frac{1}{2}g + \frac{1}{2}g = g$. By (9), $E^{m+\rho}e^s S$ is an integer $\neq 0$ and hence is numerically $\geqq 1$. But by Lemma 2 and (24),

$$|S| \leqq c_5^g V, \quad V = \left|\theta - \frac{K}{E}\right|^{\sigma - l} + \left|\theta - \frac{k}{e}\right|\ .$$

Thus

$$1 \leqq E^{m+\rho}e^s |S| \leqq c_5^g E^{m+\rho}e^s V \leqq 2c_5^g E^{m+\rho}e^s M\ ,$$

for M in (23). Define an integer c so that $2c_5^g < c^g$. This completes the proof of Lemma 4.

92. Siegel's theorems on the approximation to θ.

THEOREM 111. *Let θ satisfy an irreducible equation of degree $n \geqq 3$. Let s be a fixed one of $1, 2, \ldots, n-1$. Let*

$$(26) \qquad \nu > \frac{n}{s+1} + s\ .$$

There is only a finite number of pairs of integers x, y satisfying

$$(27) \qquad \left|\theta - \frac{x}{y}\right| < \frac{1}{y^\nu}\ , \qquad y > 0\ .$$

For $s=1$, this was proved by Thue.

I. Let the equation (7) satisfied by θ have integral coefficients and unity as its leading coefficient. It suffices to prove the theorem for integers x and y whose g.c.d. d is 1. For, if $d>1$, write $X=x/d$, $Y=y/d$. Then (27) implies

$$(28)\qquad \left|\theta-\frac{X}{Y}\right|<\frac{1}{d^{\nu}Y^{\nu}}<\frac{1}{Y^{\nu}}\,.$$

Suppose there is only a finite number of pairs of integers X and $Y(Y>0)$ for which the first term of (28) is less than the third. For each such pair, the first inequality gives an upper bound for d. Hence there will be only a finite number of pairs of integers x, y satisfying (27). We may therefore assume henceforth that x and y are relatively prime. Write

$$(29)\qquad \epsilon=\nu-\left(\frac{n}{s+1}+s\right)\,.$$

By (26), $\epsilon>0$. If the theorem is true for a given ν, it follows when ν is replaced by $h>\nu$, since $y\geqq 1$, $y^h\geqq y^\nu$. Hence we may assume that $\epsilon<1$.

Suppose there are infinitely many relatively prime solutions of (27). We have

$$\nu<\tfrac{1}{2}n+s+\epsilon<\tfrac{1}{2}n+(n-1)+1<2n\,.$$

For a fixed ϵ, choose a number δ so small that

$$(30)\qquad \frac{\delta}{s+1}+\nu\delta<\frac{\epsilon}{2}\,,\qquad 0<\delta<\tfrac{1}{2}\,.$$

To each y correspond only a finite number of integers x. Hence there is a solution with y arbitrarily large. Thus there is a solution $x=K$, $y=E$, in relatively prime integers, such that

$$(31)\qquad E>c_0,\qquad E^{\epsilon/4}>c\,.$$

For the same reason there is a relatively prime solution k, e, where e is so large that the integer g determined by

$$(32)\qquad E^g \leqq e < E^{g+1}$$

satisfies

$$(33)\qquad g \geqq 2n^2\,, \qquad \frac{g\epsilon}{4} > \nu n^2 + s\,.$$

By (31), $e > c_0^g$. There exists an integer l depending on θ, s, ϵ only which satisfies the inequalities in Lemma 4. Since K, E and k, e satisfy (27), the maximum of

$$\left(\frac{1}{E^\nu}\right)^{g-l}, \qquad \frac{1}{e^\nu}$$

exceeds M in (23). Hence

$$(34)\qquad \text{Max.}\ \{c^g E^{m+g-\nu(g-l)} e^s\,, \qquad c^g E^{m+g} e^{s-\nu}\} > 1\,.$$

By (32), (8), Lemma 4, (30) and (33),

$$E^{m+g-\nu(g-l)} e^s < E^z\,, \quad z = m+g-\nu(g-l)+(g+1)s\,,$$

$$\frac{z}{g} \leqq \frac{n+\delta}{s+1} - \nu + \frac{\nu l}{g} + s + \frac{s}{g} = \frac{\delta}{s+1} - \epsilon + \frac{\nu l}{g} + \frac{s}{g}$$

$$\leqq \frac{\delta}{s+1} - \epsilon + \frac{\nu}{g}(\delta g + n^2) + \frac{s}{g} < \tfrac{1}{2}\epsilon - \epsilon + \tfrac{1}{4}\epsilon = -\tfrac{1}{4}\epsilon\,.$$

Since $\nu > s$, (32) gives $(1/e)^{\nu-s} \leqq (1/E^g)^{\nu-s}$. Then by (8)

$$E^{m+g} e^{s-\nu} \leqq E^w\,, \qquad w = \frac{n+\delta}{s+1}\,g + g(s-\nu)\,.$$

Then by (29) and (30),

$$\frac{w}{g} = \frac{\delta}{s+1} - \epsilon < \frac{\epsilon}{2} - \epsilon < -\tfrac{1}{4}\epsilon\,.$$

Hence by (31) both of the numbers in the brackets of (34) are < 1, a contradiction.

II. Let $q\theta^n + q_1\theta^{n-1} + \ldots + q_n = 0$ be irreducible and have integral coefficients. Multiply by q^{n-1} and write $\eta = q\theta$. Then

$$\eta^n + q_1\eta^{n-1} + qq_2\eta^{n-2} + \ldots + q^{n-1}q_n = 0 ,$$

which is of type (7). We shall be led to a contradiction if we assume that (27) has solutions with y sufficiently large. For, if we denote qx by X, we have

$$\left|\eta - \frac{X}{y}\right| < \frac{q}{y^\nu} < \frac{1}{y^p} , \qquad p = \frac{n}{s+1} + s + \frac{\epsilon}{2} ,$$

when $y^{\epsilon/2} > q$. This contradicts case (I) of Theorem 111.

To prove Theorem 108, apply Theorem 111 with

$$s = 1 , \qquad \nu = \tfrac{1}{2}n + 1 + \epsilon , \qquad \epsilon = \tfrac{1}{4}n - \tfrac{1}{2} .$$

Then for y large and every x,

$$y^\epsilon \geqq A , \qquad \left|\theta - \frac{x}{y}\right| \geqq \frac{1}{y^\nu} = \frac{y^\epsilon}{y^n} \geqq \frac{A}{y^n} .$$

THEOREM 112. *If θ satisfies an irreducible equation of degree $n \geqq 3$ and if $A > 0$,*

$$\left|\theta - \frac{x}{y}\right| < \frac{A}{y^{2\sqrt{n}}}$$

has only a finite number of integral solutions x, $y > 0$.

Let b denote $n/(s+1) + s$ for $s = [\sqrt{n}]$. Since $1 + s > \sqrt{n}$, $b < 2\sqrt{n}$. Apply Theorem 111 with $\nu = b + \epsilon$, $\epsilon = \tfrac{1}{2}(2\sqrt{n} - b)$. Then for y large and every x,

$$y^\epsilon \geqq A , \qquad \left|\theta - \frac{x}{y}\right| \geqq \frac{1}{y^\nu} \geqq \frac{A}{y^{\nu+\epsilon}} = \frac{A}{y^{2\sqrt{n}}} .$$

93. Siegel's generalization of Theorem 107. We may replace $H = c$ by $H = G$ provided the degree of G is not too large; the exact statement is

THEOREM 113. *Define $f(z)$ and $H(x, y)$ as in Theorem 107. Let M be the minimum $n/(s+1)+s$ for $s=1, \ldots, n-1$. Let $G(x, y)$ be a polynomial with integral coefficients in each term of which the sum of the exponents of x and y is $<n-M$. Then $H(x, y)=G(x, y)$ has only a finite number of integral solutions.*

We saw that $M<2\sqrt{n}$. Since $n \geqq 3$, the case $s=1$ shows that $M<n$.

I. Consider solutions with $|x| \leqq y>0$. By the degrees of the terms of G, a sufficiently small positive ϵ may be chosen so that

$$(35) \qquad |G(x, y)| \leqq C_1 y^{n-M-2\epsilon} ,$$

where C_1 (and $C_2, \ldots, C_5$ below) is >0 and free of x, y. Since

$$(36) \qquad H(x, y)=a_n(x-\theta_1 y) \ldots (x-\theta_n y)=G(x, y) ,$$

there is at least one value of k for which

$$|x-\theta_k y|<C_2 y^v , \qquad v=\frac{n-M-2\epsilon}{n} .$$

For every $j \neq k$, $|\theta_k-\theta_j|$ exceeds a constant C_3, and

$$(37) \quad |x-\theta_j y| = |(\theta_k-\theta_j)y+(x-\theta_k y)|>C_3 y-C_2 y^v>C_4 y ,$$

for y sufficiently large. From (35), (36), and the product of (37) for all $j \neq k$, we see that

$$|x-\theta_k y|<\frac{C_1 y^{n-M-2\epsilon}}{|a_n|(C_4 y)^{n-1}}=\frac{C_5}{y^{M+2\epsilon-1}} .$$

Hence if $y^\epsilon > C_5$,

$$\left|\theta_k-\frac{x}{y}\right|<\frac{C_5}{y^{M+2\epsilon}}<\frac{1}{y^{M+\epsilon}} .$$

But for y sufficiently large this contradicts Theorem 111 Hence $H=G$ has only a finite number of integral solutions with $|x| \leqq y>0$.

II. We employ the irreducible function $(-1)^n f(-z)$, to which corresponds $H(x, -Y)$. By (I), $H(x, -Y)=G(x, -Y)$ has only a finite number of integral solutions with $|x| \leqq Y>0$. Hence the same is true of $H(x, y)=G(x, y)$, $|x| \leqq |y|$, $y<0$. Next, if $|x| \leqq |y|=0$, then $x=0$.

III. We employ the irreducible polynomial

$$z^n f\left(\frac{1}{z}\right)=a_0 z^n+\ldots+a_n,$$

to which corresponds a function of x and y equal to $H(y, x)$. By (I) and (II), $H(y, x)=G(y, x)$ has only a finite number of integral solutions with $|x| \leqq |y|$. Hence the same is true of $H(x, y)=G(x, y)$, $|x| \geqq |y|$.

94. Coefficients of the factors of a reducible polynomial.

THEOREM 114. *Let two polynomials with integral coefficients*

$$\alpha(x)=a_l x^l+\ldots+a_0, \qquad \beta(x)=b_m x^m+\ldots+b_0$$

have the product $\alpha\beta=c_{l+m}x^{l+m}+\ldots+c_0$. Let A denote the g.c.d. of the coefficients of α, B that of β, and C that of $\alpha\beta$. Then $AB=C$.

I. Let $A=B=1$. Suppose that $C>1$. Then there is a prime p which divides every c_t. Let p divide $a_0, \ldots, a_{j-1}$, but not a_j. Let p divide $b_0, \ldots, b_{k-1}$, but not b_k. The cases $j=0$, $k=0$ are not excluded. Evidently c_{j+k} is

$$\ldots+a_{j+2}b_{k-2}+a_{j+1}b_{k-1}+a_j b_k+a_{j-1}b_{k+1}+a_{j-2}b_{k+2}+\ldots.$$

Every term except $a_j b_k$ is divisible by p. Hence p does not divide c_{j+k}. This contradiction shows that $C=1$.

II. For any A, B, write $a(x)=\alpha(x)/A$, $b(x)=\beta(x)/B$. Then the g.c.d. of the coefficients of $a(x)$ is 1, likewise that of $b(x)$. Hence by (I) the g.c.d. of the coefficients of ab is 1, whence that of $\alpha\beta$ is AB.

THEOREM 115 (Gauss). *If a polynomial $f(x)$ with integral coefficients is reducible, it is a product of two polynomials of degrees $\geqq 1$ with integral coefficients.*

In case the g.c.d. d of the coefficients of $f(x)$ is >1, we apply the following proof to $f(x)/d$ instead of $f(x)$. Hence let $d=1$. We have $f\equiv g\cdot h$ where g and h have rational coefficients. We may choose positive integers G and H such that the coefficients of $Gg(x)=\alpha(x)$ and $Hh(x)=\beta(x)$ are integers. We apply Theorem 114 and note that $\alpha\beta=GHf$ implies $C=GH$. Hence f is the product of α/A and β/B.

95. Thue's generalization of his Theorem 107.

THEOREM 116. *Theorem* 107 *holds also if we omit the assumption that $f(z)=0$ is irreducible, but assume that all its roots are distinct, and* $c\neq 0$.*

New proof is needed only when $f(z)$ is reducible. Then by Theorem 115, $f=\alpha(x)\ \beta(x)$, where α and β are polynomials of degrees $a>0$, $b>0$ with integral coefficients. Let $A(x, y)$ and $B(x, y)$ be the corresponding homogeneous polynomials. Our equation $H(x, y)=c$ becomes $AB=c$. For integers x and y, both A and B have integral values. Also, c is a product of two integers in only a finite number of ways. Hence if u and v are given integers $\neq 0$, it remains only to prove that

$$A(x, y)=u\ , \qquad B(x, y)=v$$

have only a finite number of common integral solutions. Since this is true when $y=0$, let $y\neq 0$, $z=x/y$. As in (3),

(38) $$y^a\alpha(z)=u\ , \qquad y^b\beta(z)=v\ ,$$

$$v^a y^{ab}\alpha^b(z)=v^a u^b=u^b y^{ab}\beta^a(z)\ ,$$

$$D=v^a\alpha^b(z)-u^b\beta^a(z)=0\ .$$

Since no root of $\alpha(z)=0$ is a root of $\beta(z)=0$, D is not identically zero. Hence there is either no rational root of $D=0$

* If $f(z)=z^3-1$, $c=0$, then $x^3-y^3=0$ has infinitely many integral solutions.

or only a finite number of rational roots. For a fixed z, (38) hold for at most two integers y, and then $x=yz$.

96. A rational approximation to any real number.

THEOREM 117. *If a is real and g is a positive integer, we can find integers x, y such that*

$$|x-ay|<\frac{1}{g}, \qquad 1\leqq y\leqq g .$$

Given av, where also v is real, we can evidently find an integer u such that $0\leqq u-av<1$. Hence $u-av$ lies in one of the g sets of numbers separated by consecutive terms of

$$0 \quad \frac{1}{g} \quad \frac{2}{g} \quad \frac{3}{g} \quad \ldots \quad \frac{g-1}{g} \quad \frac{g}{g}=1 ,$$

where the first set includes 0, but not $1/g$, and likewise for the remaining sets. Give to v the values $0, 1, \ldots, g$. Since we have $g+1$ values of $u-av$ and only g sets, at least two values lie in the same set. Let $u-av$ and $u'-av'$ lie in the kth set, so that

$$\frac{k-1}{g}\leqq u-av<\frac{k}{g}, \qquad \frac{k-1}{g}\leqq u'-av'<\frac{k}{g}, \qquad v'\neq v .$$

We may take $v'>v$. Then

$$-\frac{1}{g}<u'-av'-(u-av)<\frac{1}{g} .$$

Then $x=u'-u$ and $y=v'-v$ are the desired integers. In particular, $|a-x/y|<1/y^2$.

97. Quadratic function made an nth power.

THEOREM 118.* *If a, b, c, d are integers, $a\neq 0$, $d\neq 0$, $b^2-4ac\neq 0$, $n\geqq 3$, there is only a finite number of integral solutions of*

(39) $$aY^2+bY+c=dx^n .$$

* Thue, *Archiv for Math. og Naturv.*, Vol. XXXIV (1917), No. 16; Landau and Ostrowski, *Proc. London Math. Soc.*, XIX (1921), 276–80 (by theory of ideals); Landau, *Zahlentheorie*, III, 60–64.

Write $y=2aY+b$, $k=b^2-4ac$, $l=4ad$. Then

(40) $$y^2-k=lx^n\ ,\quad kl\neq 0,\quad n\geqq 3\ .$$

It suffices to prove that (40) has only a finite number of integral solutions, when k and l are integers.

I. Let $k=m^2$. Let $x\neq 0$. Then $y\pm m\neq 0$. Let a prime p divide $y+m$, but not $2ml$. Since p does not divide $y-m$ or l, it divides $y+m$ exactly as often as it divides x^n. Hence

$$y+m=\pm p_1^{r_1}\ .\ .\ .\ p_j^{r_j}\,z^n\ ,$$

where $p_1, \ldots, p_j$ are the distinct primes which divide $2ml$, while $r_1, \ldots, r_j$ are integers $\geqq 0$, and z is an integer. Since p_i^n may be combined with z^n, we may assume that each r_i is one of $0, 1, \ldots, n-1$. Hence $y+m=qz^n$, where q is one of a finite set of integers $\neq 0$. Similarly, $y-m=sw^n$, where s is one of a finite set of integers $\neq 0$. Hence it suffices to show that for fixed $n\geqq 3$, $q\neq 0$, $s\neq 0$, $m\neq 0$, the equation

$$qz^n-sw^n=2m$$

has only a finite number of integral solutions z, w. This is true by Theorem 116 since $f(z)=qz^n-s=0$ has distinct roots.

II. Let k be not the square of an integer. Then $x\neq 0$ in (40). We shall prove that (40) has only a finite number of integral solutions with $x>0$. Applying that result to the equation derived from (40) by replacing l by $(-1)^n l$, we obtain our theorem for (40) with $x<0$.

Hence let $x>0$. By Theorem 117,

$$\left|a-\frac{r}{q}\right|<\frac{1}{gq}\ ,\quad 1\leqq q\leqq g$$

has integral solutions r, q. We take $a=y/x$, $g=[\sqrt{x}]$. Then $\sqrt{x}<g+1\leqq 2g$, and

(41) $$1\leqq q\leqq \sqrt{x}\ ,\qquad \left|\frac{y}{x}-\frac{r}{q}\right|<\frac{2}{q\sqrt{x}}\ .$$

Write

(42) $$s=qy-rx\ .$$

Then

(43) $$s\equiv qy \pmod{x}\ ,\qquad |s|<2\sqrt{x}\ .$$

Let θ be a fixed root of $\theta^2=k$. Define K so that

(44) $$|\theta|=K=\sqrt{|k|}\ .$$

Write

$$\xi=s+q\theta\ ,\qquad t=\left(\frac{s^2-kq^2}{x}\right)^n\ ,\qquad \beta=\frac{(s-q\theta)^n(y+\theta)}{x^n}\ .$$

Since $q\neq 0$ and k is not a square, $t\neq 0$. Then

(45) $$t(y+\theta)=\beta\xi^n\ .$$

By (43) and (40),

$$s^2-kq^2\equiv q^2(y^2-k)\equiv q^2lx^n\equiv 0 \pmod{x}\ ,$$

whence t is an integer. By (42) and $\theta^2=k$,

$$s-q\theta=q(y-\theta)-rx\ ,$$
$$(s-q\theta)^n=(-1)^n r^n x^n+(y-\theta)(C+D\theta)\ ,$$

where C and D are integers. Multiply this by $y+\theta$ and apply (40). Hence $\beta=A+B\theta$, where A and B are integers.

For fixed n, k, l, each of t, A, B has a finite set of values. For, by (43) and (41),

$$|t|\leqq\left(\frac{s^2+|k|q^2}{x}\right)^n<\left(\frac{4x+|k|x}{x}\right)^n=(4+|k|)^n\ ,$$

$$|y|\leqq\sqrt{|k|+|l|x^n}\leqq x^{n/2}\sqrt{|k|+|l|}\ ,\qquad |y|+|\theta|\leqq x^{n/2}M$$
$$M=\sqrt{|k|+|l|}+K\ ,$$
$$|s|+q|\theta|<2\sqrt{x}+\sqrt{x}K=\sqrt{x}(2+K)\ .$$

Hence for both signs,

$$|A \pm B\theta| = \left| \frac{(s \mp q\theta)^n (y \pm \theta)}{x^n} \right| < (2+K)^n M .$$

But the sum and difference of $A+B\theta$ and $A-B\theta$ give $2A$ and $2\theta B$, whence A and B are limited.

Hence for fixed n, k, l, (45) includes only a finite number of equations in the unknown integers y, s, q (the last two from ξ). Also,

$$t(y \pm \theta) = (A \pm B\theta)(s \pm q\theta)^n ,$$

whence

$$(46) \qquad 2t = \{(A+B\theta)(s+q\theta)^n - (A-B\theta)(s-q\theta)^n\}/\theta .$$

For fixed n, $t \neq 0$, A and B, (46) is a Diophantine equation for s and q, since its second member is evidently a polynomial in s and q with integral coefficients. We shall prove that it has only a finite number of integral solutions.

I. Let $B \neq 0$. The coefficient of s^n is $2B \neq 0$. Also, the corresponding equation in $z = s/q$ is

$$f(z) = \{(A+B\theta)(z+\theta)^n - (A-B\theta)(z-\theta)^n\}/\theta = 0,$$

or

$$\left(\frac{z+\theta}{z-\theta}\right)^n = Q , \qquad Q = \frac{A-B\theta}{A+B\theta} \neq 0 .$$

Hence $f(z)=0$ has n distinct roots. Theorem 116 applies.

II. Let $B=0$, $E = A(1-(-1)^n)\theta^{n-1} \neq 0$. This E is the coefficient of q^n. To see that Theorem 116 applies with x and y interchanged, we note that the corresponding equation in $Z = q/s$ is

$$A(1+Z\theta)^n - A(1-Z\theta)^n = 0 , \qquad \left(\frac{1+Z\theta}{1-Z\theta}\right)^n = 1 ,$$

whose roots are distinct.

III. Let $B=0$, $E=0$. Then s and q divide $2t$.

Hence in each case (46) has only a finite number of solutions s, q. For each solution, (45) has a single unknown y. For each solution y, (40) holds for at most one integer $x>0$.

Landau employed Farey fractions in his proof. Our proof uses the simpler Theorem 117.

If $P(x)$ is of degree k and has integral coefficients and no multiple root, then $P(x)=cy^2$ has only a finite number of integral solutions.*

EXERCISE XXXVIII

1. Prove Theorem 107 when we assume only that $c\neq 0$ and that $f(z)/a_n$ is neither the nth power of a linear function nor the $\frac{1}{2}n$th power of an irreducible, quadratic function, each function having rational coefficients. Use Theorems 107 and 116.

2. Contrast in detail the theorems of this chapter with those of chapters iv and vi.

* Proof by algebraic numbers in *Jour. London Math. Soc.*, I (1926), 66–68; for $k=3$, *Proc. London Math. Soc.*, XXI (1923), 415–19. In *Messenger Math.*, LI (1922), 169–71, Mordell gave a proof for $k=3$ by using Theorem 107 for $n=4$ and the finiteness of the classes of binary quartics with given invariants.

CHAPTER XI

MINIMA OF REAL INDEFINITE BINARY QUADRATIC FORMS

98. Representation by $f(x, y)$ will be understood to be by use of integers x and y not both zero. For example, x^2+xy-y^2 represents 1, but not 0.

THEOREM 119. *Let $L(f)$ denote the lower bound of the absolute values of the numbers represented by any real indefinite binary quadratic form of discriminant d. Then always $L(f) \leqq \sqrt{d/5}$, while evidently $L(f_0)=\sqrt{d/5}$ for*

$$(1) \qquad f_0=\sqrt{d/5}(x^2+xy-y^2) .$$

If $L(f)=\sqrt{d/5}$, then f is equivalent to f_0.

Hence if f has a minimum, the latter is $\leqq \sqrt{d/5}$.

We employ the notations* of § 65. Write $R=\sqrt{d}$. Then

$$(2) \quad F_i+S_i=\frac{R}{A_{i+1}}, \qquad F_i-S_i=\frac{B_i}{A_{i+1}}, \qquad F_iS_i=\frac{A_i}{A_{i+1}}$$

$$(3) \quad F_i=(g_i\ g_{i+1}\ g_{i+2}\ \ldots) , \quad S_i=(0\ g_{i-1}\ g_{i-2}\ \ldots) ,$$

where the g_i are positive integers and each $A_i>0$. Write

$$(4) \qquad K_i=F_i+S_i .$$

The theorem will follow if we prove that, for every set of positive integers

$$(5) \qquad \ldots , g_{-1}, g_0 , g_1 , \ldots ,$$

there exists an integer i such that $K_i \geqq \sqrt{5}$. For then $A_{i+1} \leqq R/\sqrt{5}$. But by Theorem 86, the lower bound of the A_j is $L(f)$.

* In chap. vii we assumed that neither root of f is rational. But a form f having a rational root evidently takes the value zero for integers x and y not both zero. Our theorem is true trivially for such an f.

If any $g_i \geqq 3$, then $K_i > F_i > g_i$ gives $K_i > \sqrt{5}$. It remains to consider sets (5) having every $g_i = 1$ or 2.

If every $g_i = 1$, then

$$F_i = (1, F_i), \quad F_i^2 = F_i + 1, \quad F_i = \tfrac{1}{2}(\sqrt{5}+1),$$

$$S_i = \frac{1}{F_i} = \tfrac{1}{2}(\sqrt{5}-1), \quad F_i - S_i = 1, \quad F_i S_i = 1, \quad K_i = \sqrt{5}.$$

By (2), $B_i = A_{i+1} = A_i = R_i \sqrt{5}$. Since

(6) $$\Phi_i = (-1)^i A_i x^2 + B_i xy - (-1)^i A_{i+1} y^2,$$

Φ_0 is the form (1).

Next, let a certain $g_i = 2$. Then $F_i > 2$ and

$$\frac{1}{S_i} = (g_{i-1}, \ldots) < g_{i-1} + 1 \leqq 3, \qquad K_i > 2\tfrac{1}{3} > \sqrt{5}.$$

This proves Theorem 119. It is supplemented by

THEOREM 120. *If f is not equivalent to f_0, then $L(f) \leqq \sqrt{d/8} = L(f_1)$, where*

(7) $$f_1 = \sqrt{d/8}\,(x^2 + 2xy - y^2).$$

If f is equivalent to neither f_0 nor f_1, then $L(f) \leqq 5\sqrt{d/221} = L(f_2)$, where

(8) $$f_2 = \sqrt{d/221}\,(5x^2 + 11xy - 5y^2).$$

If $L(f) = L(f_i)$, then f is equivalent to f_i.

It suffices to prove that, for every set (5), such that not every $g_i = 1$, there exists an integer i for which $K_i \geqq \sqrt{8}$ or $K_i \geqq \sqrt{221/25}$ in the respective parts of the theorem. Since both inequalities hold if $K_i \geqq 3$, we may assume henceforth that every $K_i < 3$. Then every g_i is 1 or 2.

If every $g_i=2$, then

$$F_i=(2, F_i)\ , \quad F_i^2=2F_i+1\ , \quad F_i=\sqrt{2}+1\ ,$$

$$S_i=\frac{1}{F_i}=\sqrt{2}-1\ , \quad K_i=\sqrt{8}\ , \quad B_i=2A_{i+1}\ ,$$

$$A_i=A_{i+1}=\frac{R}{\sqrt{8}}\ , \quad \Phi_0=f_1\ .$$

Henceforth let both 1 and 2 occur among the g's. If three consecutive g's are 1, $g_i=2$, 1, then Theorem 82 gives

$$K_i=(2, 1, \ldots)+(0, 1, \ldots)>(2, 1, 1)+(0, 1, 1)=2\tfrac{1}{2}+\tfrac{1}{2}\ .$$

Hence no triple 1, 2, 1 occurs.

If a triple $g_i=2$, 1, 2 occurs, then $g_{i-1}=2$ by the last remark, and

$$K_i=(2, 1, 2, \ldots)+(0, 2, \ldots)>(2, 1, 2)+(0, 2, 1)=2\tfrac{2}{3}+\tfrac{1}{3}\ .$$

We shall write t_j for a succession of j terms each t.

If no term 2 precedes a 1, the set is $1_\infty\ 2_\infty$. Denote the first 2 by g_i. Then by the cases having every $g_i=1$ or every $g_i=2$,

$$K_i=(2_\infty)+(0, 1_\infty)=\sqrt{2}+1+\tfrac{1}{2}(\sqrt{5}-1)>3\ .$$

It therefore remains to treat only the case in which there is an i such that

(9) $$g_{i-1}=g_i=2\ , \qquad g_{i+1}=g_{i+2}=1\ .$$

Write $F=F_{i+3}$, $S=S_{i-1}$. We have the identity

(10) $$(0, 2, x)+(0, 1, 1, x)=1 \qquad \text{if } x>0\ .$$

Hence for $z>0$,

(11) $$(0, 2, x)+(2, z)\leqq 3 \text{ if and only if } z\geqq(1, 1, x)\ .$$

By (9), $K_i=(2, 1, 1, F)+(0, 2, 1/S)$. In (11) take $x=1/S$, $z=(1, 1, F)$. Hence $K_i\leqq 3$ if and only if $F\geqq 1/S$.

Next, $K_{i-1}=(2, 2, 1, 1, F)+S$. Add $2-2$ to (11) and take $x=(1, 1, F)$, $z=1/S$. Hence $K_{i-1}\leqq 3$ if and only if $1/S\geqq(1_4, F)$. We may therefore assume that

$$F\geqq\frac{1}{S}\geqq(1_4, F)\geqq\left(1_4, \frac{1}{S}\right). \tag{12}$$

The final quantity is $\geqq(1_8, 1/S)\geqq(1_{12}, 1/S)\geqq \ldots$, whence

$$\frac{1}{S}\geqq(1_\infty)=\tfrac{1}{2}(\sqrt{5}+1), \qquad S\leqq\tfrac{1}{2}(\sqrt{5}-1),$$

$$S_i=\left(0, 2, \frac{1}{S}\right)=\frac{1}{2+S}\geqq\tfrac{1}{2}(3-\sqrt{5}),$$

$$F_i>(2, 1, 1)=2\tfrac{1}{2}, \qquad K_i>\tfrac{1}{2}(8-\sqrt{5})>\sqrt{8}.$$

This proves the first statement in Theorem 120 and the fact that when $L(f)=\sqrt{d/8}$, f is equivalent to f_1.

Finally, let f be equivalent to neither f_0 nor f_1. Then our sets (5) have properties (9)–(12).

We next prove that the number of terms 1 which immediately follow any term 2 is even or infinite. Let $g_v=2$, 1_m, 2 occur. Here $m>1$, since 2, 1, 2 was excluded. We have $(2, \ldots)>2>\tfrac{1}{2}(\sqrt{5}+1)=(1_\infty)$. If m were odd,

$$F=(1_{m-2}, 2, \ldots)<(1_{m-2}, 1_\infty)=(1_\infty).$$

But, by (12), $F\geqq(1_4, F)\geqq(1_8, F)\geqq \ldots \geqq(1_\infty)$. This contradiction shows that m is even. It follows that the number of terms 1 which immediately precede any term 2 is even or infinite.

The chain for $\Phi_0=[5, 11, -5]$ has the period Φ_0, $\Phi_1=[-5, 9, 7]$, $\Phi_2=[7, 5, -7]$, $\Phi_3=[-7, 9, 5]$, and the δ's of the transformations $\begin{pmatrix} 0 & 1 \\ -1, & \delta \end{pmatrix}$ which replace each by the next and Φ_3 by Φ_0 are 2, -1, 1, -2. But $g_k=(-1)^k\delta_k$. Hence

$g_{4n} = g_{4n+3} = 2$, $g_{4n+1} = g_{4n+2} = 1$ for every n. Write A for F_0, B for S_0. Hence

$$A = (2, 1, 1, 2, A) = \frac{13A+5}{5A+2}, \qquad A = \frac{\sqrt{221}+11}{10},$$

$$B = (0, \dot{2}, 1, 1, \dot{2}) = \frac{1}{A} = \frac{\sqrt{221}-11}{10},$$

$$A+B = \tfrac{1}{5}\sqrt{221}.$$

We shall prove that for every set (5) there exists an i such that $K_i \geqq A+B$.

I. Let three consecutive terms 1 occur. Let $g_i = 2$ precede these three terms 1 and hence four terms 1. Then $F_i = (2, 1, 1, 1, \ldots) > A$. Also, $g_{i-1} = 2$, since a triple 1, 2, 1 is excluded. If $g_{i-2} = 2$, $S_i = (0, 2, 2, \ldots) > B$, $K_i > A+B$. Henceforth let $g_{i-2} = 1$. Hence $g_{i-3} = 1$, since 2, 1, 2 is excluded.

I₁. Let $g_{i-4} = 1$. Since an even number of terms 1 precede a term 2, $g_{i-5} = 1$. Then $S = (0, 1_4, \sigma)$, $\sigma = (g_{i-6}, \ldots)$. By (12), $S \leqq (0, 1_4, F)$. Hence $\sigma \geqq F$. Thus

$$S_i = (0, 2, 1_4, \sigma) \geqq (0, 2, 1_4, F) = \frac{5F+3}{13F+8} = \frac{13G+8}{34G+21},$$

where $G = F_{i+5}$, whence $F = (1, 1, G) = (2G+1)/(G+1)$. Hence

$$F_i = (2, 1_4, G) = \frac{13G+8}{5G+3}, \quad K_i \geqq f, \quad f = \frac{3(13G+8)^2}{\Delta},$$

where $\Delta = (5G+3)(34G+21)$. We find that

$$\frac{df}{dG} = \frac{-3(13G+8)(29G+18)}{\Delta^2}.$$

Hence f decreases when G increases, and its least value is given by $G = \infty$. Thus

$$K_i \geqq \frac{3 \cdot 13^2}{5 \cdot 34} > \tfrac{1}{5}\sqrt{221}.$$

I_2. Let $g_{i-4}=2$. Then $S_i=(0, 2, 1, 1, 2, \ldots)$ exceeds the preceding S_i, whence K_i exceeds the preceding K_i.

II. Let three consecutive terms 2 occur. Denote the last such term by $g_i=2$. By I, the set is $\ldots, 2, 2, 2, 1, 1, 2, 2, \ldots$. Hence

$$F_i>(2, 1, 1, 2, 2)=\tfrac{31}{12}\,, \quad S_i>(0, 2, 2)=\tfrac{2}{5}\,, \quad K_i>\tfrac{1}{5}\sqrt{221}\,.$$

By I and II, pairs of terms 1 alternate with pairs of terms 2. For $i=4n$, we saw before I that $F_i=A$, $S_i=B$. By means of (2) we find that Φ_i is f_2 in (8).

The preceding proofs of Theorems 119 and 120 are due to the author. But Markoff* had given an elaborate proof of an extension of Theorem 120 to an infinitude of forms $f_0, f_1, \ldots$, each having a minimum $>\frac{1}{3}R$ and such that every f having $L(f)>\frac{1}{3}R$ is equivalent to one of the f_i. An exposition will be given in the author's *Studies in the Theory of Numbers* (University of Chicago Press).

* *Mathematische Annalen*, XV (1879), 381–406; XVII (1880), 379–99.

INDEX

PRINTED IN U S A